DIGITAL AV DATA TRANSMISSION UNIT, DIGITAL AV DATA RECEPTION UNIT, DIGITAL AV DATA TRANSMISSION/RECEPTION SYSTEM AND MEDIUM

Patent number: JP2000059323

Publication date: 2000-02-25

Inventor: NISHIMURA TAKUYA; IIZUKA HIROYUKI; YAMADA MASAZUMI; GOTO SHOICHI; TAKECHI HIDEAKI; USUKI NAOJI

Applicant: MATSUSHITA ELECTRIC IND CO LTD

Classification:

- international: H04H1/00; H04L9/08; H04L9/10; H04L29/08; H04N7/167

- european:

Application number: JP19980224825 19980807

Priority number(s):

Also published as:

EP0977436 (A1

WO9941910 (A

EP0977436 (A4

Abstract of **JP2000059323**

PROBLEM TO BE SOLVED: To appropriately perform data communication while being immune to forge or alteration and considering the importance of data or class of a recognition method by receiving an authentication request and performing authentication based on one kind of authentication rule selected out of a means storing plural authentication rules on the side of transmission based on the discriminated result of a data importance discriminating means.

SOLUTION: When an authentication requesting means 12 receives the authentication request, a data importance discriminating means 3 discriminates the importance of AV data 2 to be transmitted and classifies them according to CGMS values. A transmission side authentication selecting means 6 sends the optimum authentication rule, which is selected out of a means 5 storing plural authentication rules on the side of transmission, to a digital AV reception unit TV9. At a digital AV transmission unit STB1, the same authentication rule as the selected certification rule is selected and a reception side authentication means 13 and a transmission side authentication means 7 mutually perform the authentication. When th authentication is made successful, the AV data 2 to be transmitted are enciphered and transmitted while using a work key Kco16 and the received enciphered data are deciphered by a work key Kco17.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－59323
（P2000－59323A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.⁷	識別記号	FI		テーマコード(参考)
H04H 1/00		H04H 1/00	F	
H04L 9/08		H04L 9/00	601B	
9/10			621	
29/08		13/00	307Z	
H04N 7/167		H04N 7/167	Z	

審査請求　未請求　請求項の数43　ＯＬ　（全 28 頁）

(21)出願番号　特願平10－224825

(22)出願日　平成10年８月７日(1998.8.7)

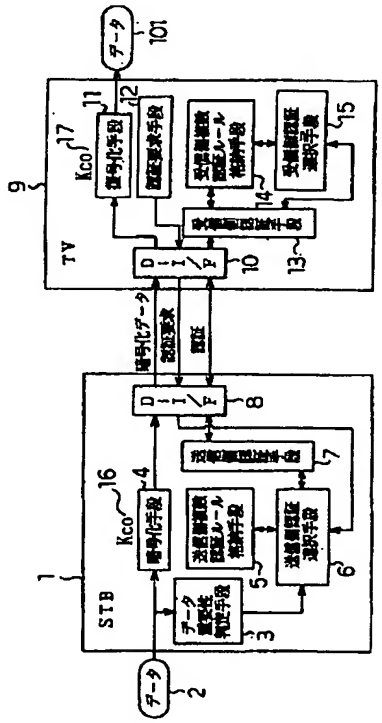
(31)優先権主張番号　特願平10－31847
(32)優先日　平成10年２月13日(1998.2.13)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平10－151586
(32)優先日　平成10年６月１日(1998.6.1)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　西村　拓也
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　飯塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100092794
弁理士　松田　正道

最終頁に続く

(54)【発明の名称】　デジタルＡＶデータ送信ユニット、デジタルＡＶデータ受信ユニット及び、デジタルＡＶデータ送受信システム、媒体

(57)【要約】
【課題】　重要でないデータの認証に多くの時間を要したり、重要なデータであるにもかかわらずその認証が偽造や改竄に弱い。また、ユニットによって認証に必要な厳密さが異なる。
【解決手段】　データ２の重要度を判定するデータ重要性判定手段３、その判定結果に基き送信側複数認証ルール格納手段５から一種類のルールを選択する送信側認証選択手段６及び、その選択された認証ルールに基づき認証を行う送信側認証手段７を有するＳＴＢ１と、認証要求を行う認証要求手段１２、送信側で選択された認証ルールと同じ認証ルールを受信側複数認証ルール格納手段１４から選択する受信側認証選択手段１５及び、その選択された認証ルールに基づき認証を行う受信側認証手段１３を有するＴＶ９とを備える。



1

【特許請求の範囲】

【請求項１】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項２】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ受信ユニット。

【請求項３】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルＡＶデータ受信ユニットとを備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項４】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、所定の管理基準を格納した管理基準格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

2

【請求項５】　前記送信ユニットは前記受信ユニットの各機能を有し、前記受信ユニットは前記送信ユニットの各機能を有することを特徴とする請求項３記載のデジタルAVデータ送受信システム。

【請求項６】　前記受信ユニットの機能を有する送信ユニット、あるいは前記送信ユニットの機能を有する受信ユニットが三つ以上互いに接続され、デジタルAVデータを互いにやりとりできることを特徴とする請求項５記載のデジタルAVデータ送受信システム。

【請求項７】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶ送信ユニット。

【請求項８】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ受信ユニット。

【請求項９】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ル

ール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、
前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有するデジタルＡＶデータ受信ユニットと、を備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項１０】　所定の管理基準を格納した管理基準格納手段と、デジタルＡＶデータ受信ユニットから認証要求を受けて、そのデジタルＡＶデータ受信ユニットの種類又は重要度に応じて、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルＡＶ送信ユニット。

【請求項１１】　前記管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リスト（ＣＲＬ）であることを特徴とする請求項４又は１０に記載のデジタルＡＶ送信ユニット。

【請求項１２】前記送信ユニットに、前記受信ユニットが二つ以上接続され、前記送信ユニットとの間で、デジタルＡＶデータをやりとりできることを特徴とする請求項９記載のデジタルＡＶデータ送受信システム。

【請求項１３】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項１４】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットと、
前記認証の要求を行う認証要求手段と、前記送信側認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有する複数認証デジタルＡＶデータ受信ユニットと、
認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側単一認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記デジタルＡＶデータ送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有する単一認証デジタルＡＶデータ受信ユニットと、を備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項１５】前記複数認証デジタルＡＶデータ受信ユニットは前記デジタルＡＶデータ送信ユニットの各機能を有し、前記デジタルＡＶデータ送信ユニットは前記複数認証デジタルＡＶデータ受信ユニットの各機能を有することを特徴とする請求項１４記載のデジタルＡＶデータ送受信システム。

【請求項１６】前記複数認証デジタルＡＶデータ受信ユニットの各機能を有するデジタルＡＶデータ送信ユニット、あるいは前記デジタルＡＶデータ送信ユニットの機能を有する複数認証デジタルＡＶデータ受信ユニットが二つ以上互いに接続され、且つ、前記単一認証デジタルＡＶデータ受信ユニットが二つ以上接続され、デジタルＡＶデータを互いにやりとりできることを特徴とする請求項１５記載のデジタルＡＶデータ送受信システム。

【請求項１７】　デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等及びそれ以下のレベルの前記解読情報を、前記受信ユニットに送信

する解読情報選択手段とを備えたことを特徴とする送信ユニット。

【請求項１８】　データの重要度に応じた複数のレベルで暗号化されたデジタルＡＶデータを送信する送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等及びそれ以下のレベルの前記暗号化データに対する解読情報を、前記送信ユニットに要求する解読情報要求手段とを備えたことを特徴とする受信ユニット。

【請求項１９】　デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等及びそれ以下のレベルの前記解読情報を、前記受信ユニットに送信する解読情報選択手段とを有する送信ユニットと、
その送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等及びそれ以下のレベルの解読情報を、前記送信ユニットに要求する解読情報要求手段とを有する受信ユニットとを備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項２０】　デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等またはそれ以下のレベルの解読情報を前記受信ユニットに送信する解読情報選択手段とを備え、前記解読情報選択手段は、次に前記受信ユニットから解読情報の要求があった時に、その要求が前記判定済みの認証レベルと同等あるいはそれ以下のレベルの前記解読情報の場合は、前記認証手続きを行わずに要求された解読情報を前記受信ユニットに送信することを特徴とする送信ユニット。

【請求項２１】　データの重要度に応じた複数のレベルで暗号化されたデジタルＡＶデータを送信する送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等またはそれ以下のレベルの前記暗号化データに対する解読情報を前記送信ユニットに要求する解読情報要求手段とを備え、前記解読情報要求手段は、前記認証のレベルと同等あるいはそれ以下のレベルの解読情報を前記送信ユニットに要求する時は、前記認証要求を行わずに、前記解読情報の要求を行うことを特徴とする受信ユニット。

【請求項２２】　デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等またはそれ以下のレベルの解読情報を前記受信ユニットに送信する解読情報選択手段とを有し、前記解読情報選択手段は、次に前記受信ユニットから解読情報の要求があった時に、その要求が前記判定済みの認証レベルと同等あるいはそれ以下のレベルの前記解読情報の場合は、前記認証手続きを行わずに要求された解読情報を前記受信ユニットに送信する送信ユニットと、
その送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等またはそれ以下のレベルの解読情報を前記送信ユニットに要求する解読情報要求手段とを備え、前記解読情報要求手段は、前記認証のレベルと同等あるいはそれ以下のレベルの解読情報を前記送信ユニットに要求する時は、前記認証要求を行わずに、前記解読情報の要求を行う受信ユニットとを備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項２３】　受信側ユニットから送られてきた認証要求について、認証を行い、又、その認証のレベルを判定し、そのレベルと同等な認証方法及びそれより低いレベルの認証方法に対応する暗号化方法のそれぞれの解読情報を、前記受信側ユニットからの解読情報の要求に応じて、前記受信側ユニットへ送信することを特徴とするデジタルＡＶデータ送信方法。

【請求項２４】　受信側ユニットから送られてきた解読情報要求について、その要求された解読情報に対応する認証のレベルを判定し、そのレベルと前記受信側ユニットとの間で過去に実行した認証のレベルとを比較し、前記判定された認証のレベルが過去の認証のレベルと同等もしくはより低いレベルの場合は、前記受信側ユニットから前記要求された解読情報を送信することを特徴とするデジタルＡＶデータ送信方法。

【請求項２５】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から１種類の認証ルールを選択する送信側認

証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットであって、
認証の要求を行い、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段から１種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ受信ユニットまたは、前記送信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、前記重要度の判定を行ったユニットが重要度の判定を行わないユニットに前記選択した認証ルールについての情報を送り、前記重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択することを特徴とするデジタルＡＶデータ送信ユニット。

【請求項２６】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段から１種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ送信ユニットに対して、認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記受信側複数認証ルール格納手段から１種類の認証ルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたデジタルＡＶデータ受信ユニットであって、前記送信ユニットまたは受信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、前記重要度の判定を行ったユニットが重要度の判定を行わないユニットに前記選択した認証ルールについての情報を送り、前記重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択することを特徴とするデジタルＡＶデータ受信ユニット。

【請求項２７】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から１種類の認証ルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、
前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記受信側複数認証ルール格納手段から１種類の認証ルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルＡＶデータ受信ユニットとを備え、前記送信ユニットまたは受信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、前記重要度の判定を行ったユニットが重要度の判定を行わないユニットに前記選択した認証ルールについての情報を送り、前記重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択することを特徴とするデジタルＡＶデータ送受信システム。

【請求項２８】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証の要求を行い、デジタルＡＶデータの重要度を判定してその判定結果に基づいて、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段から一種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ受信ユニットで選択される前記認証ルールと同じルールを、前記送信側複数認証ルール格納手段から選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項２９】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段から受信側で選択される所定の認証ルールと同じ認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ送信ユニットに対して、認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、そのデータ重要性判定手段の判定結果に基づいて、前記受信側複数認証ルール格納手段から一種類の認証ルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ受信ユニット。

【請求項３０】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から受信側で選択される所定の認証ルールと同じルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、
前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、そのデータ重要性判定手段の判定結果に基づいて、前記受信側複数認証ルール格納手段から一種類のルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルＡＶデータ受信ユニットとを備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項３１】　複数種類の認証ルールから１種類の認証ルールを選択して認証を行う認証手段と、受信ユニットに対する所定の管理基準を格納した管理基準格納手段と、前記受信ユニットからの認証要求を受け、前記格納されている管理基準を参照することにより認証するか否

かを判定する認証判定手段とを備えたデジタルＡＶデータ送信ユニットであって、前記認証要求を行う受信ユニットが、前記管理基準を持てない重要度の低い認証ルールのみで認証する機能しか有しない場合に、前記受信ユニットは、外部の管理センターからその受信ユニットに対応する前記管理基準用の識別情報が付与されるものであり、前記送信ユニットの認証判定手段は、前記認証要求の際に前記識別情報を受け取り、その識別情報が不可となった場合に、前記認証を取りやめることを特徴とするデジタルＡＶデータ送信ユニット。

【請求項３２】　受信ユニットからの認証要求を受け、管理基準格納手段に格納されている受信ユニットに対する所定の管理基準を参照することにより認証するか否かを判定する認証判定手段を有するデジタルＡＶデータ送信ユニットに対し、前記認証要求を行う認証要求手段と、前記管理基準を持てない重要度の低い認証ルールのみで認証する認証手段とを備え、外部の管理センターから受信ユニット自身に対応する前記管理基準用の識別情報が付与されるデジタルＡＶデータ受信ユニットであって、前記送信ユニットの認証判定手段は、前記認証要求の際に前記識別情報を受け取り、その識別情報が不可となった場合に、前記認証を取りやめることを特徴とするデジタルＡＶデータ受信ユニット。

【請求項３３】　複数種類の認証ルールから１種類の認証ルールを選択して認証を行う認証手段と、受信ユニットに対する所定の管理基準を格納した管理基準格納手段と、前記受信ユニットからの認証要求を受け、前記格納されている管理基準を参照することにより認証するか否かを判定する認証判定手段とを有するデジタルＡＶデータ送信ユニットと、その送信ユニットに対し、前記認証要求を行う認証要求手段と、前記管理基準を持てない重要度の低い認証ルールのみで認証する認証手段とを有し、外部の管理センターから受信ユニット自身に対応する前記管理基準用の識別情報が付与されるデジタルＡＶデータ受信ユニットとを備え、前記送信ユニットの認証判定手段は、前記認証要求の際に前記識別情報を受け取り、その識別情報が不可となった場合に、前記認証を取りやめることを特徴とするデジタルＡＶデータ送受信システム。

【請求項３４】　前記所定の管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リストであり、前記識別情報が、前記受信ユニットに対応する前記管理基準用のＩＤおよびそのＩＤに対する署名であることを特徴とする請求項３１記載のデジタルＡＶデータ送信ユニット。

【請求項３５】　前記認証判定手段は、前記ＩＤ及び署名の少なくと一方が不可となった場合に、前記認証を取りやめることを特徴とする請求項３４記載のデジタルＡＶデータ送信ユニット。

【請求項３６】　前記署名は、受信ユニットそれぞれにあらかじめ固有に付加されている識別ＩＤを利用して作成されるものであることを特徴とする請求項３４、または３５記載のデジタルＡＶデータ送信ユニット。

【請求項３７】　前記所定の管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リストであり、前記識別情報が、前記受信ユニットに対応する前記管理基準用のＩＤおよびそのＩＤに対する署名であることを特徴とする請求項３２記載のデジタルＡＶデータ受信ユニット。

【請求項３８】　前記認証判定手段は、前記ＩＤ及び署名の少なくと一方が不可となった場合に、前記認証を取りやめることを特徴とする請求項３７記載のデジタルＡＶデータ受信ユニット。

【請求項３９】　前記署名は、受信ユニットそれぞれにあらかじめ固有に付加されている識別ＩＤを利用して作成されるものであることを特徴とする請求項３７、または３８記載のデジタルＡＶデータ受信ユニット。

【請求項４０】　前記所定の管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リストであり、前記識別情報が、前記受信ユニットに対応する前記管理基準用のＩＤおよびそのＩＤに対する署名であることを特徴とする請求項３３記載のデジタルＡＶデータ送受信システム。

【請求項４１】　前記認証判定手段は、前記ＩＤ及び署名の少なくと一方が不可となった場合に、前記認証を取りやめることを特徴とする請求項４０記載のデジタルＡＶデータ送受信システム。

【請求項４２】　前記署名は、受信ユニットそれぞれにあらかじめ固有に付加されている識別ＩＤを利用して作成されるものであることを特徴とする請求項４０、または４１記載のデジタルＡＶデータ送受信システム。

【請求項４３】　請求項１～４２のいずれかに記載のユニット又はシステムもしくは送信方法が有する各構成要素もしくはステップが持つ機能の全部又は一部を実現するためのプログラムを格納したことを特徴とする媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＡＶ装置間において認証を行う機能を持つＡＶシステムに関するものである。

【０００２】

【従来の技術】従来のＡＶ装置間において認証を行うシステムについて図２と図３を用いて説明する。

【０００３】まず、図２において、デジタルＡＶデータ送信ユニットＳＴＢ１８は、公開鍵と秘密鍵２０、認証手段１９、デジタルインターフェースＤ－Ｉ／Ｆ２２、暗号化手段１９を備えている。その公開鍵と秘密鍵２０は、認証手段１９を介して、デジタルインターフェースＤ－Ｉ／Ｆ２２に接続している。また、暗号化手段１９は、公開鍵と秘密鍵２０を参照することが出来、デジタ

ルインターフェース２２に接続している。デジタルＡＶデータ受信ユニットＴＶ２３も公開鍵と秘密鍵２６、認証手段２５、デジタルインターフェースＤ－Ｉ／Ｆ２４、復号化手段２７を具備している。その公開鍵と秘密鍵２６は認証手段２５を介してデジタルインターフェースＤ－Ｉ／Ｆ２４に接続している。また、復号化手段２７は公開鍵と秘密鍵２６を参照することが出来、デジタルインターフェースＤ－Ｉ／Ｆ２４に接続している。さらにデジタルインターフェースＤ－Ｉ／Ｆ２２とデジタルインターフェースＤ－Ｉ／Ｆ２４は互いにデータのやり取りが出来る構成となっている。

【０００４】次にデジタルＡＶデータ送信ユニットＳＴＢ１８とデジタルＡＶデータ受信ユニットＴＶ２３間の動作を説明する。まず、デジタルＡＶデータ受信ユニットＴＶ２３が認証要求を出す。するとデジタルインターフェースＤ－Ｉ／Ｆ２４を通してデジタルＡＶデータ送信ユニットＳＴＢ１８を構成するデジタルインターフェースＤ－Ｉ／Ｆ２２に認証要求が到達する。デジタルインターフェースＤ－Ｉ／Ｆ２２は認証要求を受けて認証手段１９にて、公開鍵と秘密鍵２０を参照して認証する。デジタルＡＶデータ送信ユニットＳＴＢ１８にて認証されれば、暗号化手段２１において、データが暗号化されて、デジタルインターフェースＤ－Ｉ／Ｆ２２を介して、暗号化したデータが送信される。これはデジタルインターフェースＤ－Ｉ／Ｆ２４を介して、公開鍵と秘密鍵２６を参照して、復号化手段２７で復号される。

【０００５】このようにすると、偽造や改竄に強い機能が実現出来る。しかし、公開鍵と秘密鍵を用いた認証は多くの時間を要する。ニュースのように、あまり重要でないデータの場合、不必要に認証に時間を取られることがある。またＶＴＲのようにコピー可能なデータしか受け取っては機器は、場合によってデジタルＡＶデータ受信ユニットが厳密な認証を要しないこともあり、そのような場合、時間の無駄が生じる。

【０００６】次に、図３において、デジタルＡＶ送信ユニットＳＴＢ２８は共通鍵３０、認証手段２９、デジタルインターフェースＤ－Ｉ／Ｆ３２、暗号化手段３１を具備している。その共通鍵３０は、認証手段２９を介して、デジタルインターフェースＤ－Ｉ／Ｆ３２に接続している。また、暗号化手段３１は、共通鍵３０を参照することが出来、デジタルインターフェース３２に接続している。デジタルＡＶデータ受信ユニットＴＶ３３も、共通鍵３６、認証手段３５、デジタルインターフェース３４、復号化手段３７を具備している。その共通鍵３６は認証手段３５を介してデジタルインターフェース３４に接続している。また、復号化手段３７は共通鍵３６を参照することが出来、デジタルインターフェース３４に接続している。さらにデジタルインターフェース３２とデジタルインターフェース３４は互いにデータのやり取りが出来る構成となっている。

【０００７】次にデジタルＡＶデータ送信ユニットＳＴＢ２８とデジタルＡＶデータ受信ユニットＴＶ３３間の動作を説明する。まず、デジタルＡＶ受信ユニットＴＶ３３が認証要求を出す。するとデジタルインターフェースＤ－Ｉ／Ｆ３４を通してデジタルＡＶ送信ユニットＳＴＢ２８を構成するデジタルインターフェースＤ－Ｉ／Ｆ３２に認証要求が到達する。デジタルインターフェースＤ－Ｉ／Ｆ３２は認証要求を受けて認証手段２９にて、共通鍵３０を参照して認証する。デジタルＡＶ送信ユニットＳＴＢ２８にて認証されれば、暗号化手段３１において、データが暗号化されて、デジタルインターフェースＤ－Ｉ／Ｆ３２を介して、暗号化したデータが送信される。これはデジタルインターフェースＤ－Ｉ／Ｆ３４を介して、共通鍵３６を参照してデジタ復号化手段３７で復号される。

【０００８】このようにすると、短い時間でデータの認証を行うことができる。しかし、共通鍵を用いた認証は偽造や改竄に弱いので、新作の映画など著作権上重要なデータの場合、第三者にデータを無料で視聴されることがある。またＴＶのように受信した全てのデータを表示するために、厳密な認証を行う機器と接続した場合に対応できる必要があり、デジタルＡＶデータ受信ユニットが厳密な認証を要する場合があり、そのような場合重要なデータの著作権が保護されないといったことが起こりうる。

【０００９】

【発明が解決しようとする課題】このように、あまり重要でないデータの認証に多くの時間を要するという課題や、重要なデータであるにもかかわらずその認証が偽造や改竄に弱いという課題が存在する。また、デジタルＡＶデータ受信ユニットによっては、厳密な認証を要しないものも存在し、このようなユニットに対して厳密な認証を行った場合、時間の無駄が生じるという課題や、逆にデジタルＡＶデータ受信ユニットによっては厳密な認証を要するものも存在し、そのようなユニットに厳密でない認証を行った場合、著作権が守られないといった課題が存在する。更に、不正使用の防止のために、厳密な認証と厳密でない認証とで、暗号鍵を各々に対応して用意した場合、厳密な認証を行って暗号鍵を取得した後に、厳密でないデータを必要とする場合でも、改めて厳密でない認証を行う必要がある。また、受信側が機器の排除機能を持たない機器の場合は、送信側は不正な機器を排除できない構成になっているという課題がある。

【００１０】本発明は、このような従来の、重要でないデータの認証に多くの時間を要するという課題と、重要なデータであるにもかかわらずその認証が偽造や改竄に弱いという課題と、ユニットによって認証に必要な厳密さが異なるといった課題を考慮し、データの重要性や相手の装置が有する認証方法の種別などを考慮して、適切な認証方法でデータの送受信を行いうるユニット、シ

ステム等を提供することを目的とするものである。

【００１１】

【課題を解決するための手段】上述した課題を解決するために、請求項１の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基き、送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットである。

【００１２】また請求項２の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基き、送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットを通信の対象とし、認証の要求を行う認証要求手段と、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたデジタルＡＶデータ受信ユニットである。

【００１３】また請求項３の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基き、送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、認証の要求を行う認証要求手段と、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルＡＶデータ受信ユニットとを備えたデジタルＡＶデータ送受信システムである。

【００１４】また請求項４の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、所定の管理基準を格納した管理基準格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基き、管理基準格納手段の管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットである。

【００１５】また請求項５の本発明は、送信ユニットは受信ユニットの各機能を有し、受信ユニットは送信ユニットの各機能を有する請求項３記載のデジタルＡＶデータ送受信システムである。

【００１６】また請求項６の本発明は、受信ユニットの機能を有する送信ユニット、あるいは送信ユニットの機能を有する受信ユニットが三つ以上互いに接続され、デジタルＡＶデータを互いにやりとりできる請求項５記載のデジタルＡＶデータ送受信システムである。

【００１７】また請求項７の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、デジタルＡＶデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶ送信ユニットである。また請求項８の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、デジタルＡＶデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットを通信の対象とし、認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側認証ルール格納手段と、認証ルールについての情報を送信する認証ルール情報送信手段と、送信ユニットとの間で認証ルールにて認証を行う受信側認証手段とを少なくとも備えたデジタルＡＶデータ受信ユニットである。

【００１８】また請求項９の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、デジタルＡＶデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、認証

の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側認証ルール格納手段と、認証ルールについての情報を送信する認証ルール情報送信手段と、送信ユニットとの間で認証ルールにて認証を行う受信側認証手段を少なくとも有するデジタルＡＶデータ受信ユニットとを備えたデジタルＡＶデータ送受信システムである。

【００１９】また請求項１０の本発明は、所定の管理基準を格納した管理基準格納手段と、デジタルＡＶデータ受信ユニットから認証要求を受けて、そのデジタルＡＶデータ受信ユニットの種類又は重要度に応じて、管理基準格納手段の管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたデジタルＡＶ送信ユニットである。

【００２０】また請求項１１の本発明は、管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リスト（ＣＲＬ）である請求項４又は１０に記載のデジタルＡＶ送信ユニットである。

【００２１】また請求項１２の本発明は、送信ユニットに、受信ユニットが二つ以上接続され、送信ユニットとの間で、デジタルＡＶデータをやりとりできる請求項９記載のデジタルＡＶデータ送受信システムである。

【００２２】また請求項１３の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、データ重要性判定手段の判定結果に基づき、送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、送信側認証選択手段又は送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットである。

【００２３】また請求項１４の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、データ重要性判定手段の判定結果に基づき、送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、送信側認証選択手段又は送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットと、認証の要求を行う認証要求手段と、送信側認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有する複数認証デジタルＡＶデータ受信ユニットと、認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側単一認証ルール格納手段と、認証ルールについての情報を送信する認証ルール情報送信手段と、デジタルＡＶデータ送信ユニットとの間で認証ルールにて認証を行う受信側認証手段を少なくとも有する単一認証デジタルＡＶデータ受信ユニットとを備えたデジタルＡＶデータ送受信システムである。

【００２４】また請求項１５の本発明は、複数認証デジタルＡＶデータ受信ユニットはデジタルＡＶデータ送信ユニットの各機能を有し、デジタルＡＶデータ送信ユニットは複数認証デジタルＡＶデータ受信ユニットの各機能を有する請求項１４記載のデジタルＡＶデータ送受信システムである。

【００２５】また請求項１６の本発明は、複数認証デジタルＡＶデータ受信ユニットの各機能を有するデジタルＡＶデータ送信ユニット、あるいはデジタルＡＶデータ送信ユニットの機能を有する複数認証デジタルＡＶデータ受信ユニットが二つ以上互いに接続され、且つ、単一認証デジタルＡＶデータ受信ユニットが二つ以上接続され、デジタルＡＶデータを互いにやりとりできる請求項１５記載のデジタルＡＶデータ送受信システムである。

【００２６】請求項１７の本発明は、デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等及びそれ以下のレベルの解読情報の全部、又は一部を、受信ユニットに送信する解読情報選択手段とを備えた送信ユニットである。

【００２７】請求項１８の本発明は、データの重要度に応じた複数のレベルで暗号化されたデジタルＡＶデータを送信する送信ユニットから受信した暗号化されたデー

タを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等及びそれ以下のレベルの暗号化データに対する解読情報の全部、又は一部を、送信ユニットに要求する解読情報要求手段とを備えた受信ユニットである。

【００２８】請求項１９の本発明は、デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等及びそれ以下のレベルの解読情報の全部、又は一部を、受信ユニットに送信する解読情報選択手段とを有する送信ユニットと、その送信ユニットから受信した暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等及びそれ以下のレベルの解読情報の全部、又は一部を、送信ユニットに要求する解読情報要求手段とを有する受信ユニットとを備えたデジタルＡＶデータ送受信システムである。

【００２９】請求項２０の本発明は、デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等のレベルの解読情報を受信ユニットに送信する解読情報選択手段とを備え、解読情報選択手段は、次に受信ユニットから解読情報の要求があった時に、その要求が判定済みの認証レベルと同等あるいはそれ以下のレベルの解読情報の場合は、認証手続きを省略して要求された解読情報を受信ユニットに送信する送信ユニットである。

【００３０】請求項２１の本発明は、データの重要度に応じた複数のレベルで暗号化されたデジタルＡＶデータを送信する送信ユニットから受信した暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等のレベルの暗号化データに対する解読情報を送信ユニットに要求する解読情報要求手段とを備え、解読情報要求手段は、認証のレベルと同等あるいはそれ以下のレベルの解読情報を送信ユニットに要求する時は、認証要求を行わずに、解読情報の要求を行う受信ユニットである。

【００３１】請求項２２の本発明は、デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等のレベルの解読情報を受信ユニットに送信する解読情報選択手段とを有し、解読情報選択手段は、次に受信ユニットから解読情報の要求があった時に、その要求が判定済みの認証レベルと同等あるいはそれ以下のレベルの解読情報の場合は、認証手続きを省略して要求された解読情報を受信ユニットに送信する送信ユニットと、その送信ユニットから受信した暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等のレベルの解読情報を送信ユニットに要求する解読情報要求手段とを備え、解読情報要求手段は、認証のレベルと同等あるいはそれ以下のレベルの解読情報を送信ユニットに要求する時は、認証要求を行わずに、解読情報の要求を行うとを有する受信ユニットとを備えたデジタルＡＶデータ送受信システムである。

【００３２】請求項２５の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から１種類の認証ルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットであって、認証の要求を行い、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段から１種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ受信ユニットまたは、送信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、重要度の判定を行ったユニットが重要度の判定を行わないユニットに選択した認証ルールについての情報を送り、重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択するデジタルＡＶデータ送信ユニットである。

【００３３】請求項２８の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証の要求を行い、デジタルＡＶデータの重要度を判定してその判定結果に基づいて、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認

証ルール格納手段から一種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ受信ユニットで選択される認証ルールと同じルールを、送信側複数認証ルール格納手段から選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットである。

【００３４】請求項３１の本発明は、複数種類の認証ルールから１種類の認証ルールを選択して認証を行う認証手段と、受信ユニットに対する所定の管理基準を格納した管理基準格納手段と、受信ユニットからの認証要求を受け、格納されている管理基準を参照することにより認証するか否かを判定する認証判定手段とを備えたデジタルＡＶデータ送信ユニットであって、認証要求を行う受信ユニットが、管理基準を持てない重要度の低い認証ルールのみで認証する機能しか有しない場合に、受信ユニットは、外部の管理センターからその受信ユニットに対応する管理基準用の識別情報が付与されるものであり、送信ユニットの認証判定手段は、認証要求の際に識別情報を受け取り、その識別情報が不可となった場合に、認証を取りやめるデジタルＡＶデータ送信ユニットである。

【００３５】請求項４３の本発明は、請求項１～４２のいずれかに記載のユニット又はシステムもしくは送信方法が有する各構成要素もしくはステップが持つ機能の全部又は一部を実現するためのプログラムを格納した媒体である。

【００３６】

【発明の実施の形態】以下に本発明の実施の形態を図面を参照して説明する。

【００３７】まず、第一の実施の形態について図１を参照して説明する。

【００３８】デジタルＡＶデータ送信ユニットＳＴＢ１は、データ重要性判定手段３、暗号化手段４、送信側複数認証ルール格納手段５、送信側認証選択手段６、送信側認証手段７及びデジタルインターフェースＤ－Ｉ／Ｆ８を持つ。このデータ重要性判定手段３は、データ２の重要性を重要度に応じて複数種類に場合分けを行う手段である。このデータの重要度はＣＧＭＳで表現されている。このＣＧＭＳは放送局から送られてくるデータの内部あるいはヘッダーに存在している。暗号化手段４は、データ２を、認証の過程で作成されたワーク鍵Ｋｃｏ１６で暗号化する手段である。ワーク鍵Ｋｃｏ１６を生成するその認証方法は後述する。送信側複数認証ルール格納手段５は、複数種類の認証ルールを持つ手段である。例えば、公開鍵と秘密鍵を用いた認証ルールと、共通鍵を用いた認証ルールの２種類の認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。送信側認証選択手段６は、送信側複数認証ルール格納手段５が持つ複数種類の認証ルールから一種類の認証ルールを選択する手段である。この際、データ重要性判定手段３の判定の結果を参考にする。本実施の形態では、前記の重要度が高いか低いかにより、時間はかかるが偽造や改竄に強い認証ルールとして、公開鍵と秘密鍵を用いた認証ルールを選択し、時間はかからないが、偽造や改竄に弱いルールとして、共通鍵を用いた認証ルールを選択する。送信側認証手段７は、選択された認証ルールで実際にデジタルＡＶデータ受信ユニットＴＶ９と認証をかわす手段である。デジタルインターフェースＤ－Ｉ／Ｆ８は、デジタルＡＶデータ受信ユニットＴＶ９とＡＶデータや信号のやりとりを行う手段である。

【００３９】デジタルＡＶデータ受信ユニットＴＶ９は、デジタルインターフェースＤ－Ｉ／Ｆ１０、復号化手段１１、認証要求手段１２、受信側認証手段１３、受信側複数認証ルール格納手段１４、受信側認証選択手段１５を持つ。この認証要求手段１２は、デジタルＡＶデータ送信ユニットＳＴＢ１に認証要求を出す手段である。また、受信側複数認証ルール格納手段１４は、送信側複数認証ルール格納手段５に格納された複数の認証ルールと同じ複数の種類の認証ルールを持つ手段である。従って本実施の形態の場合、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールを持つ。受信側認証選択手段１５は上述した受信側複数認証ルール格納手段１４から、送信側認証選択手段６で選択された認証ルールと同じ認証ルールを選択する手段である。受信側認証手段１３は、その選択された認証ルールで、つまりデジタルＡＶデータ送信ユニットＳＴＢ１で選択された認証ルールを用いて実際にデジタルＡＶデータ送信ユニットＳＴＢ１と認証を互いに交わす手段である。復号化手段１１はデジタルＡＶデータ送信ユニットＳＴＢ１で暗号化され送信されてきたデジタルＡＶデータをワーク鍵Ｋｃｏ１７を用いて復号化する手段である。ワーク鍵Ｋｃｏ１７は前記受信側認証過程で生成されるもので、その生成する方法は前記ワーク鍵Ｋｃｏ１６を生成する方法とともに後述する。デジタルインターフェースＤ－Ｉ／Ｆ１０は、送信ユニットＳＴＢ１とＡＶデータや信号のやりとりを行う手段である。

【００４０】次に、このような本実施の形態の動作を説明する。

【００４１】まず、デジタルＡＶデータ受信ユニットＴＶ９を構成する、認証要求手段１２が、デジタルインターフェースＤ－Ｉ／Ｆ１０を介して、デジタルＡＶデータ送信ユニットＳＴＢ１に自らのＩＤを含めて認証要求を出す。もちろんＡＶデータの送信要求も出す。デジタルＡＶデータ送信ユニットＳＴＢ１は、デジタルインターフェースＤ－Ｉ／Ｆ８を介して、前記認証要求を受信する。そうするとデジタルＡＶデータ送信ユニットＳＴＢ１は、まずデータ重要性判定手段３で、これから送信すべきＡＶデータ２の重要性を判定し場合分けする。す

なわちＣＧＭＳの値が１１なら重要度は高く、そのデータは表示のみ可能であり、コピーすることは禁止される。また、ＣＧＭＳの値が１０の場合は一回のみコピー可能であり、比較的重要なデータである。またＣＧＭＳが００の場合は自由に視聴ないしはコピーして使用してよいので、重要でないデータと言える。またＣＧＭＳが０１となるＡＶデータは存在しない。このＣＧＭＳの値によりデータの重要度の場合分けがなされる。この結果は送信側認証選択手段６に送られ、送信側複数認証ルール格納手段５から最適な認証ルールが選択される。すなわち、最新の映画など重要なデータの場合には、時間がかかるが、偽造や改竄に強い、公開鍵と秘密鍵を用いる認証ルールが選択される。また、ニュースのような重要でないデータの場合には、時間はかからないが、偽造や改竄に弱い、共通鍵を用いる認証ルールが選択される。更にその選択情報は、送信側認証手段７に送られ、デジタルインターフェースＤ－Ｉ／Ｆ８を介して、デジタルＡＶ受信ユニットＴＶ９に送られる。デジタルＡＶ受信ユニットＴＶ９においては、受信側認証選択手段１５が、その選択情報を利用して受信側複数認証ルール格納手段１４から、デジタルＡＶデータ送信ユニットＳＴＢ１で選択された認証ルールと同じ認証ルールを選択する。従って選択されている認証ルールは送信側と受信側とで同じになる。そこで、受信側認証手段１３と送信側認証手段７とは互いに、デジタルインタフェースＤ－Ｉ／Ｆ１０およびデジタルインタフェースＤ－Ｉ／Ｆ８を介して、認証を行う。認証が成功すれば、後述するようにして送信側にワーク鍵Ｋｃｏ１６、また受信側にワーク鍵Ｋｃｏ１７が生成される。送信すべきデータ２は生成されたワーク鍵Ｋｃｏ１６を用いて、暗号化手段４で暗号化される。そのあと、デジタルインターフェースＤ－Ｉ／Ｆ８を介して、デジタルＡＶデータ受信ユニットＴＶ９に暗号化データとして送信される。デジタルインターフェースＤ－Ｉ／Ｆ１０を介して暗号化されたデータは、ワーク鍵Ｋｃｏ１７を用いて、復号化手段１１にて復号化され、データ１０１になる。これはデータ２と同一のデータであり、デジタルＡＶデータ送信ユニットＳＴＢ１から、デジタルＡＶデータ受信ユニットＴＶ９にデータが送信されたことになる。

【００４２】最後に、デジタルＡＶデータ受信ユニットＴＶ９は、ディスプレイ装置の画面にそのデータを表示する。このようにして、データの重要性が高い時は、時間はかかるが、偽造や改竄に強い認証手段が用いられ、またデータの重要性が低い時は、時間はかからないが、偽造や改竄に弱い認証ルールが用いられる。

【００４３】次に前述したようにデジタルＡＶデータ受信ユニットＴＶ９からデジタル送信ユニットＳＴＢ１に認証要求が出たときの認証のやりとりを示し、その結果ワーク鍵Ｋｃｏを生成する実施の形態を図４と図５を参照して説明する。

【００４４】まず、図４に示すごとき、公開鍵と秘密鍵による認証を行う場合である。この場合受信側は秘密鍵Ｓｂと公開鍵Ｐｂを持つ。また送信側は秘密鍵Ｓａと公開鍵Ｐａを持つ。まずステップ１で受信側が乱数Ｂを発生する。受信側は自己の認識番号であるＩＤｂと乱数Ｂを自らの秘密鍵Ｓｂで暗号化した暗号文Ｓｂ（Ｂ）を送信側に送る。送信側は受信側の認識番号ＩＤｂから検索して受信側の公開鍵Ｐｂを入手する。ステップ８で入手した公開鍵Ｐｂで暗号文Ｓｂ（Ｂ）を復号化する。その結果ステップ９のごとく乱数Ｂが得られる。さらに、送信側は、ステップ１０のごとく乱数Ａを発生する。乱数ＡとＢは送信側の秘密鍵Ｓａで暗号化され暗号文Ｓａ（Ａ，Ｂ）が作成される。送信側は暗号文Ｓａ（Ａ，Ｂ）と自己の認識番号ＩＤａを受信側に送信する。受信側は暗号文Ｓａ（Ａ，Ｂ）と送信側の認識番号ＩＤａを受け取る。受信側は、送信側の認識番号ＩＤａから検索して送信側の公開鍵Ｐａを入手し、ステップ２のごとく、Ｐａで暗号文Ｓａ（Ａ，Ｂ）を復号化する。ここで、暗号文Ｓａ（Ａ，Ｂ）から受信側にはステップ１で送った乱数Ｂと全く同一の乱数Ｂが得られ、偽造や改竄が行われてないことが受信側にわかる。もし前記２つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。但し、この場合は、公開鍵Ｐａ，Ｐｂは正当な者にしか入手できないようになっているものとする。次に受信側はステップ３のごとく、受信側の秘密鍵Ｓｂで乱数Ａを暗号化し、暗号文Ｓｂ（Ａ）を作成する。Ｓｂ（Ａ）は送信側に送られ、ステップ１１のごとく既に送信側で持っている、受信側の公開鍵Ｐｂで暗号文Ｓｂ（Ａ）を復号化する。ステップ１０で発生した、乱数Ｂとステップ１１で復号化した乱数Ｂは全く同一であれば、偽造や改竄が行われていないことが送信側にわかる。もし前記２つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。

【００４５】今、受信側と送信側でやりとりした乱数ＡとＢは偽造や改竄が行われていないとすると、受信側と送信側以外の第３者には乱数ＡとＢは秘密の乱数である。そこで送信側で、ステップ１２のごとく、乱数ＡとＢを用いて鍵Ｋａｂを作成する。同じくステップ４のごとく受信側で乱数ＡとＢを用いて鍵Ｋａｂを作成する。前記２つのＫａｂは全く同一のものであり共通鍵となっている。次に送信側でステップ１３のごとく鍵Ｋｅｘを作成する。これを共通鍵Ｋａｂで暗号化し、暗号文Ｋａｂ（Ｋｅｘ）を作成して、受信側に送る。受信側はステップ５のごとく共通鍵Ｋａｂで暗号文Ｋａｂ（Ｋｅｘ）を復号化してＫｅｘを得、その結果、受信側が得た鍵Ｋｅｘと送信側にある鍵Ｋｅｘは全く同一であり、共通鍵となる。次に送信側でステップ１４のごとく鍵Ｋｃｏを作成する。鍵Ｋｃｏは共通鍵Ｋｅｘで暗号化され、暗号文Ｋｅｘ（Ｋｃｏ）として、受信側に送られる。受信側では、ステップ６のごと

く共通鍵Kexで暗号文Kex（Kco）を復号化し、ステップ７のごとくKcoを得る。送信側にある鍵Kcoと受信側にあるKcoは全く同一で、共通鍵となっている。以上が公開鍵と秘密鍵による認証の過程で得られたワーク鍵Kcoである。

【００４６】次に図５に示すごとき、共通鍵による認証を行う場合の説明をする。この場合、送信側と受信側は共通鍵Ｓを持つ。なお、この共通鍵は正当な者にしか与えられていない。まず,受信側でステップ１５のごとく２個の乱数Ａ１，Ａ２を発生し、共通鍵Ｓで暗号化し、暗号文Ｓ（Ａ１Ａ２）を作成し、送信側へ送る。送信側ではステップ２０のごとく共通鍵Ｓで暗号文Ｓ（Ａ１Ａ２）を復号化する。そうすると、ステップ２１のごとく乱数Ａ１と乱数Ａ２が得られる。送信側は乱数Ａ２を受信側に送る。受信側はステップ１６のごとく２つの乱数Ａ１とＡ２を持つことになる。ステップ１５で発生した乱数Ａ２とステップ１６で送信側から受け取った乱数Ａ２が全く同じであれば、送信側で偽造や改竄が行われていないことがわかる。もし、上記２つの乱数が異なっていれば偽造や改竄が行われたことになり認証は失敗する。次に送信側はステップ２２のごとく乱数Ｂ１とＢ２を発生し、暗号化して、暗号文Ｓ（Ｂ１Ｂ２）を受信側に送る。受信側はステップ１７のごとく共通鍵Ｓを用いて暗号文Ｓ（Ｂ１Ｂ２）を復号化する。すると、ステップ１８のごとく乱数Ｂ１とＢ２が得られる。受信側は乱数Ｂ２を送信側に送る。送信側はステップ２３のごとく乱数Ｂ１とＢ２を持つことになる。ステップ２２で発生した乱数と、ステップ２３で受信側から受け取った乱数Ｂ２が同じであれば、受信側に、偽造や改竄が行われていないことがわかり、認証は成功する。もし、上記２つの乱数が異なっていれば、偽造や改竄が行われたことになり認証は失敗である。

【００４７】ここまでで、認証が成功しているとすると、乱数Ａ１と乱数Ｂ１は送信側と受信側以外の第３者には秘密の乱数である。送信側ではステップ２４のごとく乱数Ａ１と乱数Ｂlから鍵Kcoを作成する。一方受信側では、ステップ１９のごとく乱数Ａ１と乱数Ｂ１から鍵Kcoを作成する。送信側にある鍵Kcoと受信側にある鍵Kcoは全く同一であり、共通鍵となっている。以上が共通鍵による認証の過程で得られたワーク鍵Kcoである。

【００４８】なお、本発明において、選択する認証ルールの種類は、前記公開鍵及び秘密鍵と共通鍵との２種類に限らず、その他の種類でもよく、更に３種類以上の異なる認証ルールを使用するものであってもよい。

【００４９】また、本実施の形態の変形例として、デジタルＡＶデータ送信ユニット１はデジタルAV受信ユニット９と同じ機能を有し、また、デジタルＡＶデータ受信ユニット９はデジタルＡＶ送信ユニット１と同じ機能を有するようになっていてもよい。以後それらのユニットのことを、デジタルＡＶデータ送受信ユニットと呼ぶ。またそれらの送受信ユニットが３台以上が互いに接続されていてもよい。

【００５０】次に本発明の第二の実施の形態について図６を参照して説明する。

【００５１】本実施の形態では、第一の実施の形態がデータの重要度に応じて認証ルールを変えていたのに対して、デジタルＡＶデータ受信ユニットＶＴＲ４５が有する認証ルールの種類によって、認証ルールを選択するところが、相違点である。

【００５２】デジタルＡＶデータ送信ユニットＳＴＢ３８は、送信側複数認証ルール格納手段４１等を持つ。送信側複数認証ルール格納手段４１は、複数種類の認証ルールを持つ手段である。これは第一の実施の形態で説明したごとく、例えば、公開鍵と秘密鍵を用いた認証ルールと、共通鍵を用いた認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。ユニット認証ルール情報受信手段４２は、デジタルＡＶデータ受信ユニットＶＴＲ４５から送られて来た認証ルールに関連する情報を受信する手段である。送信側認証取り出し手段５３は、その認証ルールに関連する情報に基づいて、送信側複数認証ルール格納手段４１から所定の認証ルールを取り出し、送信側認証手段４３に渡す手段である。送信側認証手段４３は、デジタルＡＶ受信ユニットＶＴＲ４５と互いに認証を交わす手段である。暗号化手段４０は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Kco５３により、データ３９を暗号化する手段である。デジタルインターフェースＤ－Ｕ／Ｆ４４は、デジタルＡＶデータ受信ユニットＶＴＲ４５とデータや信号のやりとりをする手段である。

【００５３】デジタルＡＶデータ受信ユニットＶＴＲ４５は、受信側認証ルール格納手段４９等を持つ。この受信側認証ルール格納手段４９は、第一の実施の形態で説明した場合とは違って、一種類の認証ルールのみ格納する手段である。例えば、公開鍵と秘密鍵を用いた認証ルール、あるいは共通鍵を用いた認証ルールのような認証ルールがある。ここで、受信側認証ルール格納手段４９に格納されている認証ルールはデジタルＡＶデータ受信ユニットＶＴＲ４５の装置の性質あるいは重要度によって、あらかじめ決められている。すなわちデータの再利用を予定しないＴＶなどのユニットには時間はかかるが、偽造や改竄に強い認証ルールが格納されており、またデータのコピーを前提とするＶＴＲのようなユニットには、時間はかからないが、偽造や改竄に弱い認証ルールが格納されている。これによって、ＡＶデータの著作権を守ることができる。本実施の形態では　デジタルＡＶデータ受信ユニットＶＴＲ４５はＶＴＲであるので、受信側認証ルール格納手段４９は共通鍵を持つものとし

て説明をする。認証ルール情報送信手段５０は、デジタルＡＶデータ受信ユニットＶＴＲ４５が受信側認証ルール格納手段４９に有する共通鍵による認証ルールに関連する情報を送信する手段である。受信側認証手段５１は、デジタルＡＶ送信ユニットＳＴＢ３８と互いに認証を交わす手段である。復号化手段４７は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Ｋｃｏ５４により、暗号化されたデータを復号化する手段である。

【００５４】次にこのような本実施の形態の動作を説明する。

【００５５】まず、デジタルＡＶデータ受信ユニットＶＴＲ４５を構成する、認証要求手段４８がデジタルインターフェースＤ－Ｉ／Ｆ４６を介して、デジタルＡＶデータ送信ユニットＳＴＢ３８に認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ３８は、デジタルインターフェースＤ－Ｉ／Ｆ４４を介して、前記認証要求を受信する。また同時に、認証ルール情報送信手段５０が、受信側認証ルール格納手段４９を参照し、格納されている認証ルール、つまり共通鍵による認証ルールに関する情報を取り出す。例えば、その共通鍵による認証ルールを示す識別子を、デジタルインターフェースＤ－Ｉ／Ｆ４６を介して、デジタルＡＶデータ送信ユニットＳＴＢ３８に送る。ユニット認証ルール情報受信手段４２が、デジタルＡＶデータ受信ユニットＶＴＲ４５から送られてきた認証ルールに関する情報、つまり共通鍵による認証ルールの識別子を、デジタルインターフェースＤ－Ｉ／Ｆ４４を介して、受け取る。さらに、この認証ルールの識別子は、送信側認証ルール取り出し手段５５に渡され、送信側複数認証ルール格納手段４１から、その認証ルールに関する情報に応じた認証ルール、つまり共通鍵による認証ルールを取り出す。その後、取り出された共通鍵による認証ルールは、送信側認証手段４３に渡される。その後、送信側認証手段４３と受信側認証手段５１は互いに、デジタルインターフェースＤ－Ｉ／Ｆ４４とＤ－Ｉ／Ｆ４６を介して、認証を交わす。認証が成功すれば、その結果、第一の実施の形態で説明したごとく、送信側にワーク鍵Ｋｃｏ５３、受信側にワーク鍵Ｋｃｏ５４が生成される。データ３９は暗号化手段４０にてワーク鍵Ｋｃｏ５３により暗号化される。暗号化されたデータはデジタルインターフェースＤ－Ｉ／Ｆ４４を介して、デジタルＡＶ受信ユニットＶＴＲ４５に送られる。デジタルインターフェースＤ－Ｉ／Ｆ４６を介して暗号化されたデータは、復号化手段４７に送られ、ワーク鍵Ｋｃｏ５４を用いて復号化され、データ５２が得られる。

【００５６】なお、本発明において、送信側の認証ルールの種類は、前記共通鍵に限らず、公開鍵及び秘密鍵、またその他の種類でもよく、更に３種類以上の異なる認証ルールを使用するものであってもよい。

【００５７】また、デジタルＡＶデータ受信ユニットは２台あり、その一つは共通鍵による認証ルールのみ有し、他の一つは公開鍵及び秘密鍵のみを有するものであってもよい。さらに３台以上のデジタルＡＶデータ受信ユニットであってもよい。

【００５８】次に本発明の第三の実施の形態について図７を参照して説明する。

【００５９】第一の実施の形態がデータの重要度に応じて認証ルールを変えていたのに対し、また、第二の実施の形態がデジタルＡＶデータ受信ユニットの種類によって認証ルールを変えていたのに対し、本実施の形態では、データの重要度とデジタルＡＶ受信ユニットの種類の両方で認証ルールを決めるところが特徴である。

【００６０】本実施の形態では、デジタルＡＶデータ送信ユニットＳＴＢ５６と、複数認証デジタルＡＶデータ受信ユニットＴＶ６５と、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２の三種類のユニットを扱う。デジタルＡＶデータ送信ユニットＳＴＢ５６は複数認証デジタルＡＶデータ受信ユニットＴＶ６５と単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２にデータを送信するユニットである。複数認証デジタルＡＶデータ受信ユニットＴＶ６５に対しては、デジタルＡＶデータ送信ユニットＳＴＢ５６においてデータの重要度により複数種類の認証ルールを選択して、そのデータを送信する。また、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２は自らの持つ一つの認証ルールを用いてデジタルＡＶデータ送信ユニット ＳＴＢ５６とで認証を行うユニットである。

【００６１】デジタルＡＶデータ送信ユニットＳＴＢ５６は、データ重要性判定手段５７を持つ。これは、データ８２の重要性を重要度に応じて複数種類の場合分けを行う手段である。この重要度は第一の実施の形態で説明したごとくＣＧＭＳで表現されている。このＣＧＭＳは放送局から送られてくるデータの内部あるいはヘッダーに存在している。暗号化手段６４は、データ８２を認証の過程で作成されたワーク鍵Ｋｃｏ７９で暗号化する手段である。ワーク鍵Ｋｃｏ７９を生成する過程は第一の実施の形態で説明した。送信側複数認証ルール格納手段６３は、複数種類の認証ルールを持つ。例えば、公開鍵と秘密鍵を用いた認証ルールや、共通鍵を用いた認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。送信側認証選択手段５９は、送信側複数認証ルール格納手段６３が持つ複数種類の認証ルールから一種類の認証ルールを選択する手段である。この時、データ重要性判定手段５７の場合分けの結果を参考にする。第一の実施の形態のごとく、本実施の形態では、前記の重要度が高いか低いかにより、時間はかかるが偽造や改竄に強い認証ルールとして、公開鍵と秘密鍵を用いた認証ルールを選択し、また、時間はかからないが、偽造や改竄に弱い認証ルールとして、共通鍵を用いた認証

ルールを選択する。ユニット認証ルール情報受信手段６０は、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から送られて来た認証ルールに関する情報を受信する手段である。送信側認証ルール取り出し手段５８は、認証ルールに関連する情報に基づいて、送信側複数認証ルール格納手段６３から所定の認証ルールを取り出し、送信側認証手段６１に渡す手段である。送信側認証手段６１は、実際に複数認証デジタルＡＶデータ受信ユニットＴＶ６５及び単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２と認証を交わす手段である。デジタルインターフェースＤ－Ｉ／Ｆ６２は、複数認証デジタルＡＶデータ受信ユニットＴＶ６５や単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２とＡＶデータや信号をやりとりする手段である。

【００６２】複数認証デジタルＡＶデータ受信ユニットＴＶ６５は、認証要求手段６７を持つ。これは、デジタルＡＶデータ送信ユニットＳＴＢ５６に認証要求を出す手段である。また、受信側複数認証ルール格納手段６８は、送信側複数認証ルール格納手段６３と同じ複数種類の認証ルールを持つ。従って本実施の形態の場合、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールがある。受信側認証選択手段６９は、受信側複数認証ルール格納手段６８から、送信側認証選択手段５９で選択された認証ルールと同じ認証ルールを選択する手段である。受信側認証手段７０は、その選択された認証ルールで、つまりデジタルＡＶデータ送信ユニットＳＴＢ５６で選択された認証ルールを用いて実際にデジタルＡＶデータ送信ユニットＳＴＢ５６と認証を互いに交わす手段である。復号化手段６６は、デジタルＡＶデータ送信ユニットＳＴＢ５６で暗号化されたデジタルＡＶデータをワーク鍵Ｋｃｏ８０を用いて復号化する手段である。ワーク鍵Ｋｃｏ８０は前記認証過程で生成されるもので、その生成する方法は前記ワーク鍵Ｋｃｏ７９とともに第一の実施の形態で説明した。デジタルインターフェースＤ－Ｉ／Ｆ７１は、デジタルＡＶデータ送信ユニットＳＴＢ５６とＡＶデータや信号のやりとりを行う手段である。

【００６３】単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２は、受信側認証ルール格納手段７５を持つ。これは、前述したごとく一種類の認証ルールのみ格納する手段である。例えば、公開鍵と秘密鍵を用いた認証ルール、あるいは共通鍵を用いた認証ルールのような認証ルールがある。ここで、受信側認証ルール格納手段７５に格納されている認証ルールは単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２の装置の種類や、重要度によって、あらかじめ決められている。ここでは、受信側認証ルール格納手段７５が共通鍵を持つものとして説明をする。認証ルール情報送信手段７６は、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２が受信側認証ルール格納手段７５に有する共通鍵による認証ルールに関連する情報を送信する手段である。受信側認証手段７７は、デジタルＡＶデータ送信ユニットＳＴＢ５６と互いに認証を交わす手段である。復号化手段７３は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Ｋｃｏ８１により、暗号化されたデータを復号化する手段である。

【００６４】次にこのような本実施の形態の動作を説明する。まず、はじめに複数認証デジタルＡＶデータ受信ユニットＴＶ６５かまたは単一認証デジタルＡＶデータ受信ユニット７２が認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ５６はどのユニットから認証要求が送られて来たのかを判断する。

【００６５】以下、まず複数認証デジタルＡＶデータ受信ユニットＴＶ６５から認証要求が来た場合を説明し、次に単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から認証要求が来た場合の説明を行う。

【００６６】第一に、前述したように複数認証デジタルＡＶデータ受信ユニットＴＶ６５を構成する、認証要求手段６７が、デジタルインターフェースＤ－Ｉ／Ｆ７１を介して、デジタルＡＶデータ送信ユニットＳＴＢ５６に自らのＩＤを含めて認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ５６は、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、前記認証要求を受信する。そうするとデジタルＡＶデータ送信ユニットＳＴＢ５６は、まずデータ重要性判定手段５７で、これから送信すべきデータ８２の重要性を判定し場合分けする。この結果は送信側認証選択手段５９に送られ、送信側複数認証ルール格納手段６３から最適な認証ルールが選択される。すなわち、重要なデータの場合には、公開鍵と秘密鍵を用いる認証ルールが選択される。また、重要でないデータの場合には、共通鍵を用いる認証ルールが選択される。更にその選択情報は、送信側認証手段６１に送られ、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、複数認証デジタルＡＶデータ受信ユニットＴＶ６５に送られる。複数認証デジタルＡＶデータ受信ユニットＴＶ６５においては、受信側認証選択手段６９が、その選択情報を利用して受信側複数認証ルール格納手段６８からデジタルＡＶデータ送信ユニットＳＴＢ５６で選択された認証ルールと同じ認証ルールを選択する。従って選択されている認証ルールは送信側と受信側とで同じになる。受信側認証手段７０と送信側認証手段６１とは互いに、デジタルインターフェースＤ－Ｉ／Ｆ７１およびデジタルインターフェースＤ－Ｉ／Ｆ６２を介して、認証を行う。認証が成功すれば、第一の実施の形態で詳述したごとく、送信側にワーク鍵Ｋｃｏ７９、また受信側にワーク鍵Ｋｃｏ８０が生成される。送信すべきデータ８２は生成されたワーク鍵Ｋｃｏ７９を用いて、暗号化手段６４で暗号化される。そのあと、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、複数認証デジタルＡＶデータ受信ユニットＴＶ６５に暗号化されたデータとして送

信される。デジタルインターフェースＤ－Ｉ／Ｆ７１を介して暗号化されたデータは、ワーク鍵Ｋｃｏ８０を用いて、復号化手段６６にて復号化され、データ８３になる。これはデータ８２と同一のデータであり、デジタルＡＶデータ送信ユニットＳＴＢ５６から、複数認証デジタルＡＶデータ受信ユニットＴＶ６５にデータが送信されたことになる。このようにして、データの重要性が高い時は、時間はかかるが、偽造や改竄に強い認証ルールが用いられ、またデータの重要性が低い時は、時間はかからないが、偽造や改竄に弱い認証ルールが用いられる。

【００６７】次に単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から認証要求が来た場合の動作の説明を行う。まず、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２を構成する、認証要求手段７４がデジタルインターフェースＤ－Ｉ／Ｆ７８を介して、デジタルＡＶデータ送信ユニットＳＴＢ５６に認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ５６は、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、前記認証要求を受信する。同時に認証ルール情報送信手段７６が、受信側認証ルール格納手段７５を参照し、格納されている認証ルール、つまり共通鍵による認証ルールに関する情報を取り出す。例えば、その共通鍵による認証ルールを示す識別子を、デジタルインターフェースＤ－Ｉ／Ｆ７８を介して、デジタルＡＶデータ送信ユニットＳＴＢ５６に送る。ユニット認証ルール情報受信手段６０が、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から送られてきた認証ルールに関する情報、つまり共通鍵による認証ルールの識別子を、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、受け取り、さらにこの認証ルールの識別子は、送信側認証ルール取り出し手段５８に渡される。送信側認証ルール取り出し手段５８は、送信側複数認証ルール格納手段６３から、その認証ルールに関する情報に応じた認証ルール、つまり共通鍵による認証ルールを取り出し、送信側認証手段６１に渡す。送信側認証手段６１と受信側認証手段７７は互いに、デジタルインターフェースＤ－Ｉ／Ｆ６２とＤ－Ｉ／Ｆ７８を介して、認証を交わす。認証が成功すれば、その結果、第一の実施の形態で詳述したごとく、送信側にワーク鍵Ｋｃｏ７９、受信側にワーク鍵Ｋｃｏ８１が生成される。認証の結果ワーク鍵が生成される過程は、第一の実施の形態で詳述した。

【００６８】データ８２は暗号化手段６４にてワーク鍵Ｋｃｏ７９により暗号化される。暗号化されたデータはデジタルインターフェースＤ－Ｉ／Ｆ６２を介して、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２に送られる。デジタルインターフェースＤ－Ｉ／Ｆ７８を介して受信した暗号化されたデータは、復号化手段７３に送られ、ワーク鍵Ｋｃｏ８１を用いて復号化され、データ８４が得られる。これはデータ８２と同一のデータであり、デジタルＡＶデータ送信ユニットＳＴＢ５６から、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２にデータが送信されたことになる。

【００６９】次に、本発明の第四の実施の形態を説明する。

【００７０】本実施の形態では、デジタルＡＶデータ受信ユニットが正当なものか不正なものかを調べて作成しておいた管理基準（ＣＲＬ）を利用するものである。そのＣＲＬの作成の仕方は、例えば、消費者が購入した販売店が発行した登録カードを元に作成する方法等が考えれれる。

【００７１】図８は、その管理基準を放送局から送られてくるデジタルＡＶデータの重要度に応じて、その管理基準を参照するかどうか決定するものである。

【００７２】デジタルＡＶ送信ユニットＳＴＢ９３は、放送局から送られてくるデジタルＡＶデータの重要度に応じて、データの重要性を判定する、データ重要性判定手段８６を有する。また、データの重要度に応じて管理基準格納手段８８に格納されている管理基準情報（ＣＲＬ）を参照するかどうかを判定する、管理基準参照決定手段８７を有する。また、前記決定結果に従って、認証を行うかどうかを決定する、認証決定手段８９を有する。また、実際にデジタルＡＶデータ受信ユニットＴＶ９２と認証を交わす、認証手段９０を有する。前記認証手段９０は、デジタルインターフェースＤ－Ｉ／Ｆ９１を介して、デジタルＡＶデータ受信ユニットＴＶ９２に接続している。

【００７３】次に本実施の形態の動作を説明する。まず、放送局から送られてくるデジタルＡＶデータ８５は、データ重要性判定手段８６で、重要性を判定される。その結果は、管理基準参照決定手段８７に渡され、管理基準格納手段８８に格納されている情報を参照すべきかどうかが決定される。例えば、新作の映画等の場合は重要なので、管理基準情報を参照すると決定する。また、ニュース等の場合は重要でないので、管理基準情報を参照しないと決定する。さらに認証決定手段８９で、前記管理基準参照決定手段８７の判定決定に従って、認証すべきかどうか決定される。すなわち、デジタルＡＶデータ受信ユニットＴＶ９２が、デジタルＡＶデータ８５を受信するのに正当な機器か不当な機器かを、管理基準格納手段８８に格納されている管理基準情報で判断される。正当であると判断されれば、次の認証手段９０で、デジタルインターフェースＤ－Ｉ／Ｆ９１を介して、デジタルＡＶ受信ユニットＴＶ９２と認証が交わされる。不当と判断されればその時点で、デジタルＡＶデータ受信ユニットＴＶ９２との認証は交わされず、データ８５の送信はされない。

【００７４】他方、図９は上述した管理基準を、デジタルＡＶデータ受信ユニットの装置の種類、あるいは重要度に応じて、その管理基準を参照するかどうか決定する

ものである。

【００７５】デジタルＡＶデータ送信ユニットＳＴＢ９４は、デジタルＡＶデータ受信ユニットＶＴＲ１００の装置の種類あるいは、重要度に応じて、その管理基準格納手段９６を参照すべきかどうかを決定する、管理基準参照決定手段９５を有する。また、認証決定手段９７は、認証するかどうかを決定する。管理基準格納手段９６は、デジタルＡＶデータ受信ユニットＶＴＲ１００がデジタルＡＶデータを受信するのに正当な機器か正当でない機器かの情報が格納されている。認証手段９８は、デジタルインターフェースＤ－Ｉ／Ｆ９９を介して、デジタルＡＶデータ受信ユニットＶＴＲ１００と認証を行う。

【００７６】次に本実施の形態の動作を説明する。まず、デジタルＡＶデータ受信ユニットＶＴＲ１００が、デジタルインターフェースＤ－Ｉ／Ｆ９９を介して、管理基準参照決定手段９５に機器情報を送る。これを受けて、管理基準参照決定手段９５は、管理基準格納手段９６に格納されている情報を参照すべきかどうかを決定する。管理基準格納手段９６を参照すると決定された場合は、認証決定手段９７は、まず、管理基準格納手段９６を参照して、デジタルＡＶデータ受信ユニットがデータを受信するのに正当な機器か、不正な機器かを判定する。ここで、正当な機器と判定されれば、次の認証手段９８にて、デジタルインターフェースＤ－Ｉ／Ｆ９９を介して、デジタルＡＶデータ受信ユニットと認証を開始する。デジタルＡＶデータ受信ユニットがデータを受信するのに不正な機器と判定された場合は、認証は行われず、データの送信も行われない。

【００７７】なお、上記実施の形態では、ＳＴＢを送信ユニットとして説明してきたが、ＶＴＲで録画したデータを再生する際には、ＶＴＲが送信ユニットとなる。この際ＣＧＭＳが入力時「１回コピー可」であれば「コピー不可」に書きかえられて出力される。ここで、データの重要度としては、元の入力時における重要度と考えるべきであり、「１回コピー可」と同様の認証ルールを使うこともできる。このように「１回コピーの結果コピー不可となったデータ」と「元からコピー不可のデータ」を見分ける必要がある際には、前述した、存在しないＣＧＭＳ値０１を前者の区別用に割り当てることもできる。

【００７８】次に本発明の第五の実施の形態について説明する。

【００７９】図１０は、本発明の第五の実施の形態についての概略図である。本実施の形態では、認証手続きのレベル２段階、コンテンツの重要度、すなわち、解読情報としての暗号鍵を３種類としている。図１０において、デジタルＡＶデータ送受信システムは、送信ユニット１１１と、それに接続された受信ユニット１３０により構成されている。

【００８０】送信ユニット１１１は、コンテンツ重要度が異なるデータＡ，Ｂを各々異なる暗号鍵Ｋcoで暗号化する暗号化手段Ａ，Ｂ１１２，１１３と、暗号化用の例えば、ｃｏｐｙ＿ｎｅｖｅｒ（テープ等に記録してはいけないコンテンツ）用Ｋco、ｃｏｐｙ＿ｏｎｃｅ（一度だけ記録してもよいコンテンツ）用Ｋco、ｎｏ＿ｍｏｒｅ＿ｃｏｐｙ（これ以上コピーしてはならないコンテンツ）用Ｋcoを記憶するＫco記憶手段１１４と、受信ユニット１３０に渡す、’Ｅｘｃｈａｎｇｅ＿Ｋｅｙ’と呼ばれるｃｏｐｙ＿ｎｅｖｅｒ用、ｃｏｐｙ＿ｏｎｃｅ用、ｎｏ＿ｍｏｒｅ＿ｃｏｐｙ用の各暗号鍵Ｋexを発生するＫex発生手段１１５と、その発生した各Ｋexを記憶するＫex記憶手段１１６と、暗号化用鍵Ｋcoを所定の関数により算出する時に用いる種を発生する種発生手段１１７と、その発生した種を記憶する種記憶手段１１８と、Ｋex記憶手段１１６からのＫexと種記憶手段１１８からの種を用いて、関数Ｋco＝ｆ（種、Ｋex）によりＫcoを算出するＫco算出手段１１９と、受信ユニット１３０に対して認証手続きを実行する認証手段１２１と、受信ユニット１３０の認証済みのレベルを判定する等の処理を行うレベル判定手段１２２と、受信ユニット１３０からの種要求に対して応答する種要求コマンド応答手段１２０と、データの送受信を行うデジタルインターフェース（Ｄ－Ｉ／Ｆ）１２３により構成されている。ここで、種要求コマンド応答手段１２０及び認証手段１２１の一部などが解読情報選択手段を構成している。

【００８１】また、受信ユニット１３０は、データの送受信を行うデジタルインターフェース（Ｄ－Ｉ／Ｆ）１３１と、受信した暗号化デジタルＡＶデータのコンテンツの重要度に応じて、要求する認証のレベルを決定する要求レベル決定手段１３４と、その決定された要求レベルで、送信ユニット１１１に認証を要求し、必要な暗号鍵Ｋexを取得する認証手段１３３と、その取得したＫexを記憶するＫex記憶手段１３７と、種の要求コマンドを発行し、種を送信ユニット１１１から取得する種要求コマンド発行手段１３５と、その取得した種とＫex記憶手段１３７に記憶されたＫexとを用いて、送信ユニット１１１と同一の関数Ｋco＝ｆ（種、Ｋex）によりＫcoを算出するＫco算出手段１３６と、その算出したＫcoにより暗号化データを復号する復号化手段１３２により構成されている。ここで、種要求コマンド発行手段１３５及び認証手段１３３の一部などが解読情報要求手段を構成している。

【００８２】次に、上記実施の形態のデジタルＡＶデータ送受信システムの動作について、図面を参照しながら説明する。

【００８３】図１１において、まず、受信ユニット１３０では、要求レベル決定手段１３４が受信データのコンテンツ重要度に基づいて要求する認証のレベルを決定し、認証手段１３３に渡す。認証手段１３３はＤ－Ｉ／

Ｆ１３１を介して送信ユニットに認証要求を出す。ここでは、一番高いレベルの認証を要求するものとする。送信ユニット１１１では、Ｄ－Ｉ／Ｆ１２３を介して受け取った認証要求に基づいて認証処理を行う。認証の方法については、例えば前述した実施の形態で説明した方法等により行うことができ、このとき送信ユニット、受信ユニットともに共有の共通鍵Kabが得られる。又、このときの認証済みのレベルがレベル判定手段１２２に渡される。

【００８４】次に、認証が完了してその通知が受信ユニット１３０に送信されると、認証手段１３３は、認証レベルが最高であることから、送信ユニット１１１に対して全てのレベルのKexを要求する。ここでは、Kexのレベルとして、高い順にｃｏｐｙ＿ｎｅｖｅｒ用（Kex1）、ｃｏｐｙ＿ｏｎｃｅ用（Kex2）、ｎｏ＿ｍｏｒｅ＿ｃｏｐｙ用（Kex3）の３種類とする。

【００８５】送信ユニット１１１では、レベル判定手段１２２が、認証手段１２１から受けた要求レベルを認証済みレベルに基づいて判定し、渡せるか否かの判定と、渡せる場合は、要求のあったKex（このときは、Kex1、Kex2、Kex3）を両者が共有するKabで暗号化して、認証手段１２１を通じて受信ユニット１３０に送信する。受信ユニット１３０では、認証手段１３３が暗号化されたKab（Kex1、Kex2、Kex3）を自身の持つKabで復号してKex記憶手段１３７に記憶する。

【００８６】一方、Kex発生手段１１５が発生した各レベルのKex、すなわち、Kex1、Kex2、Kex3は、Kex記憶手段１１６に記憶され、種発生手段１１７が発生した種は、種記憶手段１１８に記憶されている。又、Kex記憶手段１１６に記憶された各Kexと、種記憶手段１１８に記憶された種とを用いて、Kco算出手段１１９が各Kco、すなわち、ｃｏｐｙ＿ｎｅｖｅｒ用（Kco1）、ｃｏｐｙ＿ｏｎｃｅ用（Kco2）、ｎｏ＿ｍｏｒｅ＿ｃｏｐｙ用（Kco3）を算出してKco記憶手段１１４に記憶している。更に、暗号化手段A，B１１２，１１３は、各データのコンテンツの重要度に対応したKcoを用いてデジタルＡＶデータを暗号化して受信ユニット１３０に送信する。

【００８７】受信ユニット１３０では、種要求コマンド発行手段１３５が種要求コマンドを送信ユニット１１１に送信する。そうすると、送信ユニット１１１では、種要求コマンド応答手段１２０が、種記憶手段１１８から種を取り出し受信ユニット１３０に送信する。ここで、図の種記憶手段１１８に現在の種及び次の種とあるのは、暗号化用のKcoを刻々と変更しているためである。

【００８８】次に、受信ユニット１３０では、種要求コマンド発行手段１３５が送信ユニット１１１から受け取った種と、Kex記憶手段に記憶している復号化するデータのレベルに対応するKexとを用いて、Kco算出手段１３６は、送信ユニット１１１と同一の関数（この関数は、送信ユニット及び受信ユニットが予め持っており、第３者は入手できないものとする）によりKcoを算出する。復号化手段１３２はこの算出されたKcoを用いて暗号化されたデジタルＡＶデータを通常のデジタルＡＶデータに復号する。ここで、利用するデータが、コンテンツ重要度の高いデータ１（例えば、映画など）から低いデータ２（例えば、スポーツ番組など）に変化、あるいは変更する場合は、最初に受け取った各Kexの中から、必要なKexを選択してKcoを算出して用いることができるので、新たな認証手続きは勿論、Kexの要求もする必要が無い。

【００８９】前述の方法は、認証手続きに続いて入手可能な全てのKexを一度に取得する方法であったが、図１２に示すような方法を用いてもよい。

【００９０】図１２において、まず、受信ユニット１３０では、要求レベル決定手段１３４が受信データのコンテンツ重要度に基づいて要求する認証のレベルを決定し、認証手段１３３に渡す。認証手段１３３はＤ－Ｉ／Ｆ１３１を介して送信ユニットに認証要求を出す。ここでは、一番高いレベルの認証を要求するものとする。送信ユニット１１１では、Ｄ－Ｉ／Ｆ１２３を介して受け取った認証要求に基づいて認証処理を行う。認証の方法については、例えば前述した実施の形態で説明した方法等により行うことができ、このとき送信ユニット、受信ユニットともに共有の共通鍵Kabが得られる。又、このときの認証済みのレベルがレベル判定手段１２２に渡される。

【００９１】次に、認証が完了してその通知が受信ユニット１３０に送信されると、認証手段１３３は、送信ユニット１１１に対して認証レベルが一番高いKexを要求する。ここでは、Kexのレベルとして、高い順にｃｏｐｙ＿ｎｅｖｅｒ用（Kex1）、ｃｏｐｙ＿ｏｎｃｅ用（Kex2）、ｎｏ＿ｍｏｒｅ＿ｃｏｐｙ用（Kex3）の３種類とする。

【００９２】送信ユニット１１１では、レベル判定手段１２２が、認証手段１２１から受けた要求レベルを認証済みレベルに基づいて判定し、渡せるか否かの判定と、渡せる場合は、要求のあったKex（このときは、Kex1）を両者が共有するKabで暗号化して、認証手段１２１を通じて受信ユニット１３０に送信する。受信ユニット１３０では、認証手段１３３が暗号化されたKab（Kex1）を自身の持つKabで復号してKex記憶手段１３７に記憶する。

【００９３】次に、受信ユニット１３０では、種要求コマンド発行手段１３５が種要求コマンドを送信ユニット１１１に送信する。そうすると、送信ユニット１１１では、種要求コマンド応答手段１２０が、種記憶手段１１８から種を取り出し受信ユニット１３０に送信する。

【００９４】種を受信した受信ユニット１３０では、種要求コマンド発行手段１３５が送信ユニット１１１から

受け取った種と、Kex記憶手段に記憶している復号化するデータのレベルに対応するKex（Kex1 ）とを用いて、Kco算出手段１３６は、送信ユニット１１１と同一の関数（この関数は、送信ユニット及び受信ユニットが予め持っており、第３者は入手できないものとする）によりKco（Kco1 ）を算出する。復号化手段１３２はこの算出されたKco1 を用いて暗号化されたデジタルＡＶデータを通常のデジタルＡＶデータに復号する。ここで、利用するデータが、コンテンツ重要度の高いデータ１から低いデータ２に変化、あるいは変更する場合は、別のKex（図ではKex2）を送信ユニット１１１に対して要求する。

【００９５】送信ユニット１１１では、レベル判定手段１２２が認証手段１２１を介して、要求されたKexのレベルを認証済みのレベルに基づいて判定し、認証済みレベルと同等か、あるいはそれより低いレベルの要求であれば、要求されたKex（Kex2）をKabで暗号化して受信ユニット１３０に送信する。

【００９６】ここで、受信ユニット１３０が、最初の認証要求を行って認証が完了した場合に、その認証済みのレベル（認証済みのレベルのうち最高のレベルのものでよい）を記憶しておき、次回からのKexの要求に対しては、その記憶した認証済みのレベルから所望するKexが認証無しに入手可能か否かを、例えば認証手段１３３で判断して入手可能であればKexを要求するようにしてもよい。このとき、入手不可能である場合は、更に、新たな高いレベルの認証を行うようにすればよい。従って、要求レベル決定手段１３４で、デジタルＡＶデータのコンテンツ重要度に基づいて決定された要求レベルが、記憶されている過去の認証済みレベルと同等かあるいはそれ以下のレベルである場合に、認証手段１３３から所望のKexを要求する。

【００９７】また、送信ユニット１１１側については、もし、認証要求がなくKexの要求があって、要求されたKexが送信不可と判定された場合に、新たな認証が必要である旨の情報を受信ユニット１３０側に通知する方法としてもよい。

【００９８】受信ユニット１３０では、認証手段１３３がKab（Kex2 ）を復号してKex記憶手段１３７に記憶し、Kco算出手段１３６がそのKex2及び種を用いてKco2を算出してデータを復号する。この方法によると、１度あるレベルでの認証が済んでいれば、そのレベルと同等か、あるいはそれ以下のレベルのKexを取得する場合、新たに認証手続きを行う必要が無いので、時間のかかる認証手続きの回数を減少することになる。

【００９９】ところで、従来のように、コンテンツの重要度の異なるＡＶデータを利用したい場合に、その都度認証手続きを行う方法では、受信ユニットが多数接続されているときは、認証要求の頻度が増大する。しかしながら、認証要求のための通信は、例えば、ＩＥＥＥ１３９４ＢＵＳ規格のようなアイソクロナスデータ通信とアシンクロナスデータ通信とを用いるものでは、本来データの通信帯域に使う帯域の一部を用いて行っているため、時間のかかる認証要求の頻度が増大することは好ましくない。従って、本実施の形態によれば、受信ユニットの台数が増えても、基本的には１受信ユニットについて１回の認証手続きで済むので、認証要求による不都合が生じない。

【０１００】なお、上記第五の実施の形態では、認証手続きのレベルを２段階としたが、これに限定されるものではない。

【０１０１】また、上記第五の実施の形態では、コンテンツの重要度のレベルを３種類としたが、これに限定されるものではない。例えば、ｃｏｐｙ＿ｆｒｅｅ（何度でも記録してよいコンテンツ）のレベルを加えて４種類としてもよいし、それ以上の種類としてもよい。

【０１０２】また、上記第五の実施の形態では、種と暗号鍵とを用いて関数により暗号化用の鍵を算出する方法により実現する構成としたが、これに限らず、他の実施の形態で説明した方法を用いた構成に適用してもよい。

【０１０３】また、上記第五の実施の形態では、受信中のデータの重要度を見て、要求するKexの種類を決定しているが、予め自分が受信する可能性のある全てのKexを取得しておいてもよい。

【０１０４】また、上記第五の実施の形態では、認証を行った後に、受信ユニットがKexの要求を行うとしたが、これに限定されない。例えば、認証要求をする際に、同時に自分が受け取りたいKexの種類を送信ユニットに対して申請し、認証が完了した時点で、送信ユニットが自動的に要求されたKexを受信ユニットに送信してもよい。

【０１０５】また、上記第五の実施の形態では、データの重要度に応じて暗号鍵を替える方法であったが、これに限らず、データの種類等に応じて暗号鍵を替えるようにしてもよい。その場合は、認証のレベルとデータの種類（すなわち、暗号鍵）を対応させておく必要がある。

【０１０６】次に本発明の第六の実施の形態について説明する。

【０１０７】図１３は、本発明の第六の実施の形態についての概略図である。本実施の形態は、Ｆｕｌｌ認証とＲｅｓｔｒｉｃｔｅｄ認証（以下，Ｒｅｓｔ認証と略称する）機能を備えたデジタルＡＶデータ送信ユニット１４０には，Ｒｅｓｔ認証機能のみを持つデジタルＡＶデータ受信ユニット１５０及びＦｕｌｌ認証とＲｅｓｔ認証の両機能を備えたデジタルＡＶデータ受信ユニット１６０が接続されているものとする。ここで、Ｆｕｌｌ認証とは、例えば公開鍵と秘密鍵とを用いた高レベルの認証方法であり、Ｒｅｓｔ認証とは、例えば共通鍵を用いた通常の認証方法を示すものとする。

【０１０８】図１３において、デジタルＡＶデータ送信

ユニット１４０は、データを暗号化する暗号化手段１４１、Ｆｕｌｌ認証用のルールを格納するＦｕｌｌ認証格納手段１４３、Ｒｅｓｔ認証用のルールを格納するＲｅｓｔ認証格納手段１４２、管理基準としてのＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ ＲｅｖｏｃａｔｉｏｎＬｉｓｔ：不正機器の排除を行うための不正機器リスト）を格納するＣＲＬ格納手段１４４、受信ユニットからの認証要求を受けて認証ルールを選択する送信側認証選択手段１４７、その送信側認証選択手段１４７の選択結果に応じて、Ｆｕｌｌ認証とＲｅｓｔ認証を切り替える切替手段１４８、切り替えられて選択された認証ルールにより受信ユニットとの間で認証を行う認証手段１４６、及び受信ユニットとの間で暗号化データや認証要求など情報のやり取りを行うＤ－Ｉ／Ｆ（デジタルインターフェース）１４５から構成されている。ＣＲＬは入力データに付加されて新しい内容に随時更新される。

【０１０９】一方、デジタルＡＶデータ受信ユニット１５０は、送信ユニットとの間で暗号化データや認証要求など情報のやり取りを行うＤ－Ｉ／Ｆ１５１、送信ユニットから受信した暗号化データを復号化する復号化手段１５２、送信ユニットに対して認証要求を行う認証要求手段１５３、及びＲｅｓｔ認証ルールにより認証を行う認証手段１５４から構成されている。

【０１１０】また、デジタルＡＶデータ受信ユニット１６０は、送信ユニットとの間で暗号化データや認証要求など情報のやり取りを行うＤ－Ｉ／Ｆ１６１、送信ユニットから受信した暗号化データを復号化する復号化手段１６２、送信ユニットに対して認証要求を行う認証要求手段１６３、Ｆｕｌｌ認証用のルールを格納するＦｕｌｌ認証格納手段１６６、Ｒｅｓｔ認証用のルールを格納するＲｅｓｔ認証格納手段１６５、認証要求手段１６３.からの指示により認証ルールを切り替える切替手段１６７、及び切り替えられ選択された認証ルールにより認証を行う認証手段１６４から構成されている。

【０１１１】次に、上記実施の形態の動作について図面を参照しながら説明する。

【０１１２】まず、前述のＣＲＬは、管理センターから送られてくるが、入手するには、Ｆｕｌｌ認証の機能を利用する。そのため、Ｒｅｓｔ認証機能のみを持つ機器では、ＣＲＬを入手できない。従って、Ｒｅｓｔ認証機能のみを持つ機器側は、ＣＲＬチェックによる機器排除を行えない。ここで、送信ユニット及び受信ユニットがともにＦｕｌｌ認証及びＲｅｓｔ認証機能を有する場合について、ＣＲＬチェックを用いた手順を説明する。

【０１１３】図１５は、図４に示した公開鍵及び秘密鍵による認証方法に、ＣＲＬチェックを付加したものである。

【０１１４】図１５において、送信側には、管理センター（ライセンス機構）からそのユニットの識別用のＩＤａ、及びそのＩＤａに対する署名Ａが送られ、受信側には、管理センターからそのユニットの識別用のＩＤｂ、及びそのＩＤｂに対する署名Ｂが送られているものとする。また、この場合受信側は秘密鍵Ｓｂと公開鍵Ｐｂを持つ。また送信側は秘密鍵Ｓａと公開鍵Ｐａを持つ。

【０１１５】まず、ステップ４１で受信側が乱数Ｂを発生する。受信側は自己の認識番号であるＩＤｂ及び署名Ｂと、乱数Ｂを自らの秘密鍵Ｓｂで暗号化した暗号文Ｓｂ（Ｂ）を送信側に送る。送信側は受信側の認識番号ＩＤｂから検索して受信側の公開鍵Ｐｂを入手する。ステップ４９で、入手した公開鍵Ｐｂで暗号文Ｓｂ（Ｂ）を復号化する。その結果ステップ５０のごとく乱数Ｂが得られる。さらに、送信側は、ステップ５１で、受信側のＩＤｂに対してＣＲＬチェックを行う。すなわち、ＩＤｂがＣＲＬに無いかどうかを調べ、無ければステップ５２で乱数Ａを発生する。ＣＲＬに有れば不正機器であるとして認証を中止する。ステップ５２で、乱数ＡとＢは送信側の秘密鍵Ｓａで暗号化され暗号文Ｓａ（Ａ，Ｂ）が作成される。送信側は暗号文Ｓａ（Ａ，Ｂ）と自己の認識番号ＩＤａを受信側に送信する。受信側は、暗号文Ｓａ（Ａ，Ｂ）と送信側の認識番号ＩＤａを受け取り、送信側の認識番号ＩＤａから検索して送信側の公開鍵Ｐａを入手し、ステップ４２のごとく、Ｐａで暗号文Ｓａ（Ａ，Ｂ）を復号化する。ここで、暗号文Ｓａ（Ａ，Ｂ）から受信側にはステップ４１で送った乱数Ｂと全く同一の乱数Ｂが得られ、偽造や改竄が行われてないことが受信側にわかる。もし前記２つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。但し、この場合は、公開鍵Ｐａ，Ｐｂは正当な者にしか入手できないようになっているものとする。次に受信側はステップ４３のごとく、受信側の秘密鍵Ｓｂで乱数Ａを暗号化し、暗号文Ｓｂ（Ａ）を作成する。Ｓｂ（Ａ）は送信側に送られ、ステップ５３のごとく既に送信側で持っている、受信側の公開鍵Ｐｂで暗号文Ｓｂ（Ａ）を復号化する。ステップ５２で発生した、乱数Ａとステップ５３で復号化した乱数Ａが全く同一であれば、偽造や改竄が行われていないことが送信側にわかる。もし前記２つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。

【０１１６】一方、受信側は、ステップ４４で送信側のＩＤａに対してＣＲＬチェックを行う。そして、ＩＤａがＣＲＬに有れば認証を中止し、無ければ次のステップに移る。今、送信側及び受信側でのＣＲＬチェックの結果が異常が無く、受信側と送信側でやりとりした乱数ＡとＢは偽造や改竄が行われていないとすると、受信側と送信側以外の第３者には乱数ＡとＢは秘密の乱数である。そこで送信側で、ステップ５４のごとく、乱数ＡとＢを用いて鍵Ｋａｂを作成する。同じくステップ４５のごとく受信側で乱数ＡとＢを用いて鍵Ｋａｂを作成する。前記２つのＫａｂは全く同一のものであり共通鍵と

なっている。次に送信側でステップ５５のごとく鍵Kexを作成する。これを共通鍵Ｋａｂで暗号化し、暗号文Ｋａｂ（Kex）を作成して、受信側に送る。受信側はステップ４６のごとく共通鍵Ｋａｂで暗号文Ｋａｂ（Kex）を復号化してKexを得、その結果、受信側が得た鍵Kexと送信側にある鍵Kexは全く同一であり、共通鍵となる。次に送信側でステップ５６のごとく鍵Kcoを作成する。鍵Kcoは共通鍵Kexで暗号化され、暗号文Kex（Kco）として、受信側に送られる。受信側では、ステップ４７のごとく共通鍵Kexで暗号文Kex（Kco）を復号化し、ステップ４８のごとくKcoを得る。送信側にある鍵Kcoと受信側にあるKcoは全く同一で、共通鍵となっている。以上が公開鍵と秘密鍵による認証の過程で得られたワーク鍵Kcoである。

【０１１７】上記説明では、ＣＲＬチェックをステップ５２の乱数Ａの発生の前に行ったが、ＩＤｂ受信後であれば、どこで行ってもよい。規格上はKABを作成するステップ５４の後に行う。

【０１１８】次に、受信側がＲｅｓｔ認証機能のみの場合について説明する。この共通鍵による認証を行う場合は、前述したような方法を用いることはできない。そこで、受信側にそのユニットに対するＣＲＬ用のＩＤとそのＩＤを用いて作成された署名を付与し、送信側でＣＲＬを利用する方法を用いる。

【０１１９】図１４において、受信側には、管理センターから受信ユニットのＩＤｂ及び署名Ｂが与えられ、送信側と受信側は共通鍵Ｓを持つ。なお、この共通鍵は正当な者にしか与えられていない。まず、受信側でステップ３０のごとく２個の乱数Ａ１，Ａ２を発生し、共通鍵Ｓで暗号化し、暗号文Ｓ（Ａ１Ａ２）を作成し、ＩＤｂ及び署名Ｂとともに送信側へ送る。送信側ではステップ３５のごとく共通鍵Ｓで暗号文Ｓ（Ａ１Ａ２）を復号化する。そして、受信側のＩＤｂに対してＣＲＬチェックを行う。また、署名Ｂもチェックする。このとき、ＣＲＬチェック及び署名Ｂのチェックのどちらか一方でも異常が有る場合は、認証を中止する。ＣＲＬチェック及び署名Ｂのチェックの結果が両方とも正常であれば、ステップ３７のごとく乱数Ａ１と乱数Ａ２が得られる。送信側は乱数Ａ２を受信側に送る。受信側はステップ３１のごとく２つの乱数Ａ１とＡ２を持つことになる。ステップ３０で発生した乱数Ａ２とステップ３１で送信側から受け取った乱数Ａ２が全く同じであれば、送信側で偽造や改竄が行われていないことがわかる。もし、上記２つの乱数が異なっていれば偽造や改竄が行われたことになり認証は失敗する。次に送信側はステップ３８のごとく乱数Ｂ１とＢ２を発生し、暗号化して、暗号文Ｓ（Ｂ１Ｂ２）を受信側に送る。受信側はステップ３２のごとく共通鍵Ｓを用いて暗号文Ｓ（Ｂ１Ｂ２）を復号化する。すると、ステップ３３のごとく乱数Ｂ１とＢ２が得られる。受信側は乱数Ｂ２を送信側に送る。送信側はステップ３９のごとく乱数Ｂ１とＢ２を持つことになる。ステップ３８で発生した乱数Ｂ２と、ステップ３９で受信側から受け取った乱数Ｂ２が同じであれば、受信側に、偽造や改竄が行われていないことがわかり、認証は成功する。もし、上記２つの乱数が異なっていれば、偽造や改竄が行われたことになり認証は失敗である。

【０１２０】ここまでで、認証が成功しているとすると、乱数Ａ１と乱数Ｂ１は送信側と受信側以外の第３者には秘密の乱数である。送信側ではステップ４０のごとくＩＤｂ及び乱数Ａ１と乱数Ｂ1から鍵Kcoを作成する。一方受信側では、ステップ３４のごとくＩＤｂ及び乱数Ａ１と乱数Ｂ１から鍵Kcoを作成する。送信側にある鍵Kcoと受信側にある鍵Kcoは全く同一であり、共通鍵となっている。以上が共通鍵による認証の過程で得られたワーク鍵Kcoである。この方法によれば、ＩＤｂと署名Ｂが対応しているので、ＩＤｂが盗まれて送信側でのＣＲＬチェックがパスしても、署名Ｂによるチェックで不正使用が防止できる。

【０１２１】ここで、ＣＲＬ用のＩＤは、例えば４０ビットのデバイスＩＤを使用する。これにより、Ｆｕｌｌ認証、Ｒｅｓｔ認証に関わらずすべての１３９４ＣＰデバイスが４０ビットのデバイスＩＤを持つことになる。

【０１２２】なお、上記の説明では、管理センターでの署名の作成を、ＩＤを用いて作成したが、このＩＤは管理センターが任意に決めるものである。さらに、安全性を高めるために、機器を製作する時に予め機器毎に埋め込まれる機器固有の識別子であるＮＵＩＤを用いる。すなわち、受信側は管理センターに申請する際に、その機器のＮＵＩＤを知らせ、管理センターは、そのＮＵＩＤとＣＲＬ用のＩＤを用いて署名を作成し、ＣＲＬ用のＩＤと署名を受信側に付与する。

【０１２３】また、上記実施の形態では、認証ルールの種類をＦｕｌｌとＲｅｓｔの２種類としたが、認証ルールの種類はこれに限定されるものではなく、３種類以上であっても、受信側がＣＲＬを持てない機器構成の場合は、前述と同様に適用可能である。

【０１２４】また、本発明の各構成要素は、それぞれの機能を実現する専用のハード回路、機器等で実現しても、あるいは、コンピュータを利用してソフトウェア的に実現してもかまわない。

【０１２５】また、本発明をコンピュータで実現する場合、それらの各構成要素の機能の全部又は一部を実現するためのプログラムを格納した媒体も本発明に属する。

【０１２６】

【発明の効果】以上説明したところから明らかなように、本発明は、重要でないデータの認証に多くの時間を要せず、重要なデータに関しては、その認証が偽造や改竄に強くまた、ユニットによって認証に必要な厳密さを変えることによって、データの重要性や相手の装置が有する認証方法の種別などを考慮して、適切な認証方法で

データの送受信を行いうるユニット、システム等を提供することができる。

【０１２７】また、本発明は、コンテンツの重要度に応じた複数種類の解読情報を得る場合に、認証回数を減少することができるという利点がある。

【０１２８】また、本発明は、排除機能を持たない受信機器であっても、送信側で機器の排除を行うことが可能となる。

【図面の簡単な説明】

【図１】本発明の第一の実施の形態についての概略図

【図２】従来技術について示す概略図

【図３】従来技術について示す概略図

【図４】本発明の実施の形態のうち認証方法に関するブロック図

【図５】本発明の実施の形態のうち認証方法に関するブロック図

【図６】本発明の第二の実施の形態についての概略図

【図７】本発明の第三の実施の形態についての概略図

【図８】本発明の第四の実施の形態についての概略図

【図９】本発明の第四の実施の形態についての概略図

【図１０】本発明の第五の実施の形態についての概略図

【図１１】同第五の実施の形態における手順方法の一例を示す図

【図１２】同第五の実施の形態における手順方法の別の一例を示す図

【図１３】本発明の第六の実施の形態についての概略図

【図１４】同第六の実施の形態における手順方法の一例を示す図

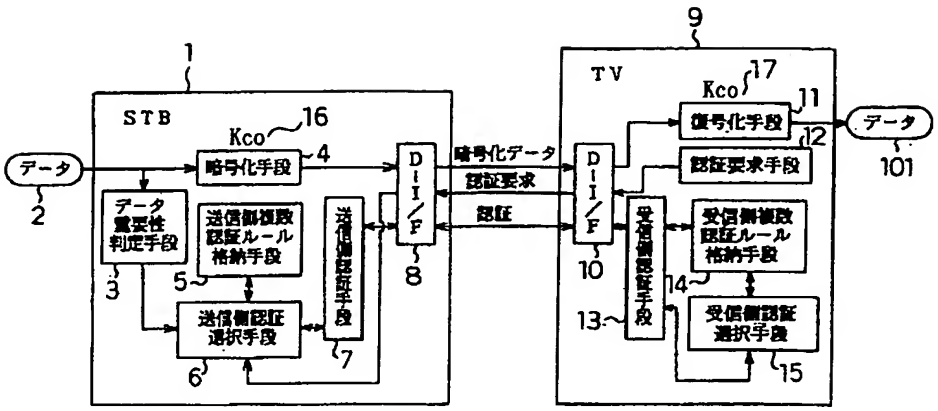
【図１５】送信側及び受信側両方でＣＲＬチェックを行う場合の手順方法の一例を示す図

【符号の説明】

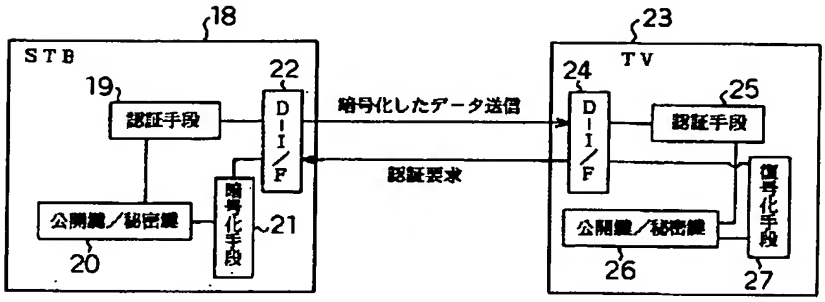
１　ＳＴＢ
３　データ重要性判定手段
５　送信側複数認証ルール格納手段
６　送信側認証選択手段
７　送信側認証手段
９　ＴＶ
１３　受信側認証手段
１４　受信側複数認証ルール格納手段
１５　受信側認証選択手段
１８　ＳＴＢ
１９　認証手段
２０　公開鍵／秘密鍵
２３　ＴＶ
２５　認証手段
２６　公開鍵／秘密鍵
２８　ＳＴＢ

＊２９　認証手段
３０　共通鍵
３３　ＴＶ
３５　認証手段
３６　共通鍵
３８　ＳＴＢ
４１　送信側複数認証ルール格納手段
４２　ユニット認証ルール情報受信手段
４３　送信側認証手段
４５　ＶＴＲ
４８　認証要求手段
４９　受信側認証ルール格納手段
５０　認証ルール情報送信手段
５１　受信側認証手段
５５　送信側認証ルール取り出し手段
５６　ＳＴＢ
５７　データ重要性判定手段
５８　送信側認証ルール取り出し手段
５９　送信側認証選択手段
６０　ユニット認証ルール情報受信手段
６１　送信側認証手段
６３　送信側複数認証ルール格納手段
６５　ＴＶ
６７　認証要求手段
６８　受信側複数認証ルール格納手段
６９　受信側認証選択手段
７０　受信側認証手段
７２　ＶＴＲ
７４　認証要求手段
７５　受信側認証ルール格納手段
７６　認証ルール情報送信手段
７７　受信側認証手段
８６　データ重要性判定手段
８７　管理基準参照決定手段
８８　管理基準格納手段
８９　認証決定手段
９０　認証手段
９２　ＴＶ
９３　ＳＴＢ
９４　ＳＴＢ
９５　管理基準参照決定手段
９６　管理基準格納手段
９７　認証決定手段
９８　認証手段
１００　ＶＴＲ
１４４　ＣＲＬ格納手段

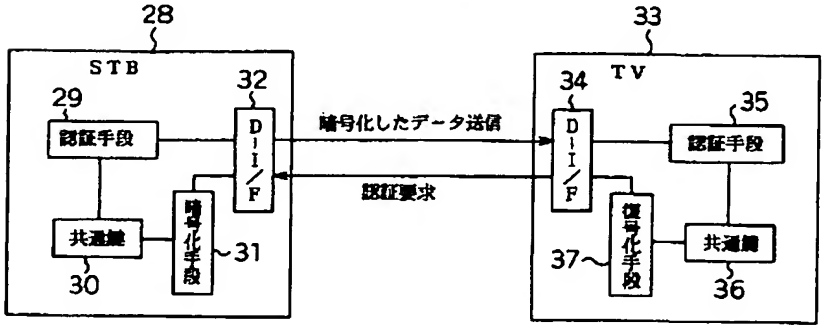
【図１】


1
STB
Kco
16
データ
2
暗号化手段
4
データ重要性判定手段
3
送信側複数認証ルール格納手段
5
送信側認証選択手段
6
送信側認証手段
7
D I / F
8
暗号化データ
認証要求
認証
9
TV
Kco
17
復号化手段
11
12
データ
101
認証要求手段
D I / F
10
受信側認証手段
13
14
受信側複数認証ルール格納手段
受信側認証選択手段
15

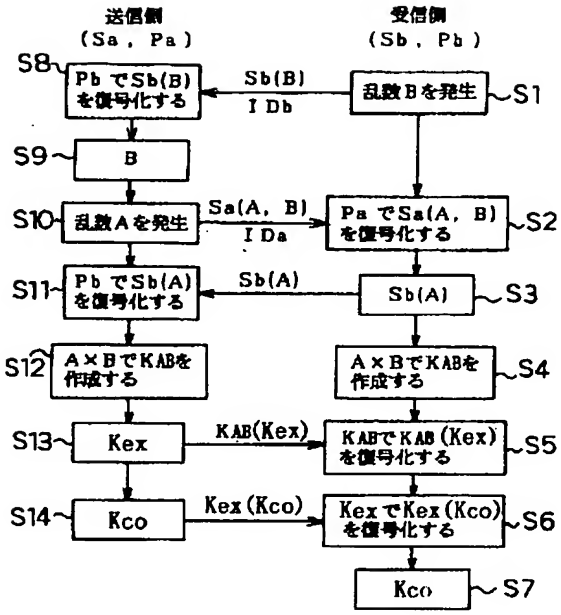
【図２】


18
STB
19
認証手段
22
D I / F
暗号化したデータ送信
認証要求
公開鍵／秘密鍵
20
暗号化手段
21
23
TV
24
D I / F
25
認証手段
公開鍵／秘密鍵
26
復号化手段
27

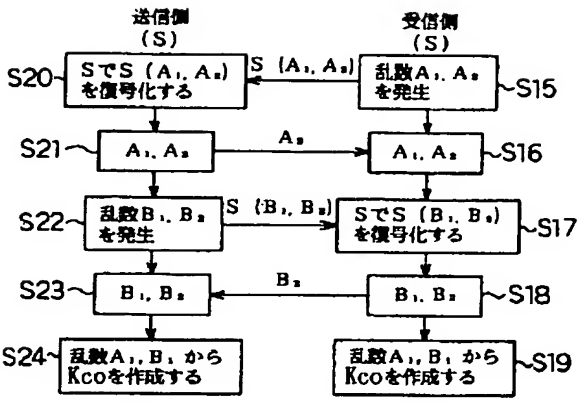
【図３】


28
STB
29
認証手段
32
D I / F
暗号化したデータ送信
認証要求
共通鍵
30
暗号化手段
31
33
TV
34
D I / F
35
認証手段
復号化手段
37
共通鍵
36

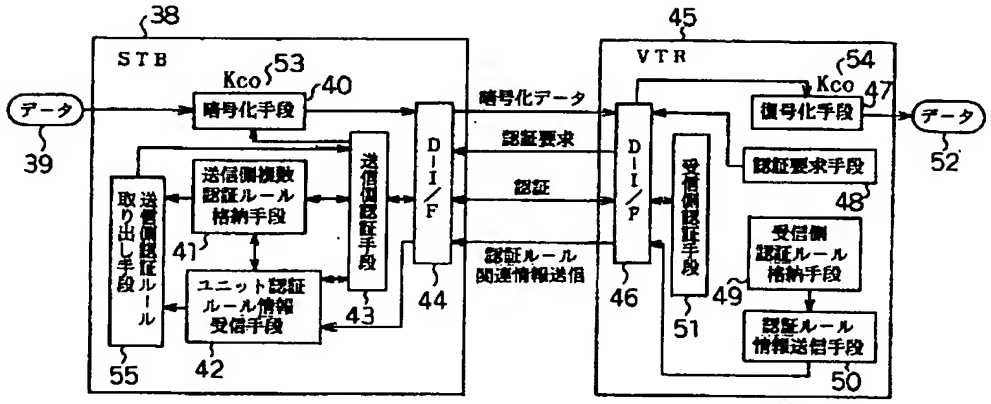
【図４】


送信側
(Sa , Pa)
受信側
(Sb , Pb)
S8
Pb でSb(B)を復号化する
Sb(B)
I Db
乱数Bを発生
S1
S9
B
S10
乱数Aを発生
Sa(A, B)
I Da
Pa でSa(A, B)を復号化する
S2
S11
Pb でSb(A)を復号化する
Sb(A)
Sb(A)
S3
S12
A×BでKABを作成する
A×BでKABを作成する
S4
S13
Kex
KAB(Kex)
KABでKAB(Kex)を復号化する
S5
S14
Kco
Kex(Kco)
KexでKex(Kco)を復号化する
S6
Kco
S7

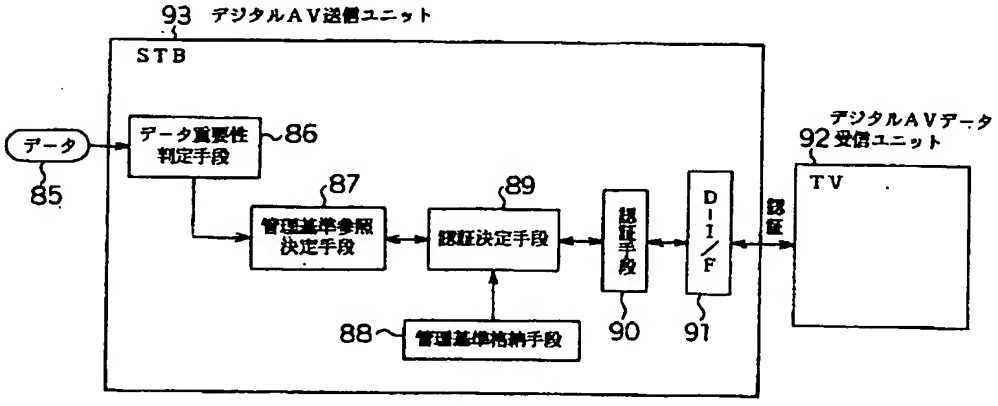
【図５】


送信側
(S)
受信側
(S)
S20
SでS(A1, A2)を復号化する
S (A1, A2)
乱数A1, A2を発生
S15
S21
A1, A2
A2
A1, A2
S16
S22
乱数B1, B2を発生
S (B1, B2)
SでS(B1, B2)を復号化する
S17
S23
B1, B2
B2
B1, B2
S18
S24
乱数A1, B1からKcoを作成する
乱数A1, B1からKcoを作成する
S19

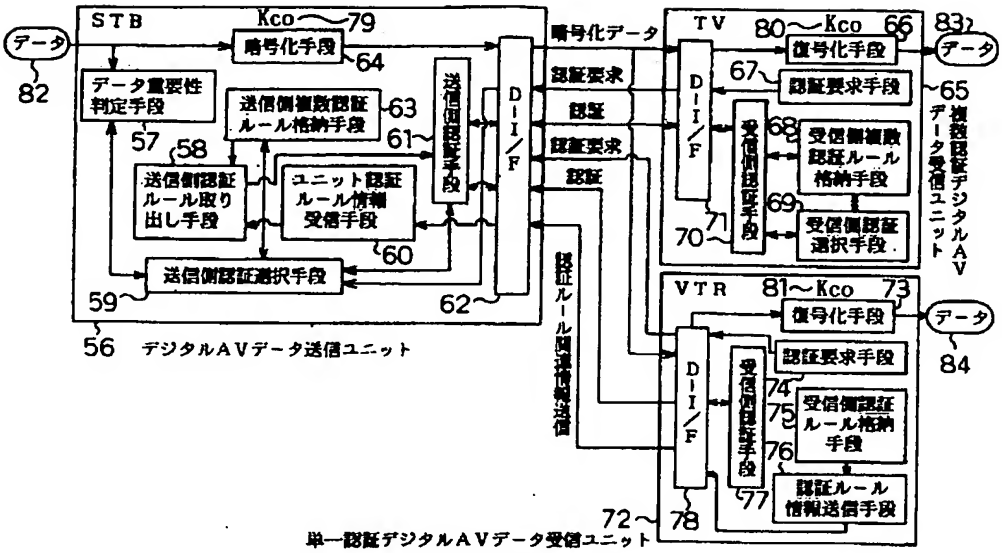
【図６】


38
STB
Kco
53
40
データ
39
暗号化手段
暗号化データ
認証要求
認証
認証ルール関連情報送信
D I / F
送信側認証手段
送信側複数認証ルール格納手段
41
ユニット認証ルール情報受信手段
43
44
送信側認証ルール取り出し手段
55
42
45
VTR
54
Kco
47
復号化手段
データ
52
認証要求手段
48
受信側認証ルール格納手段
49
認証ルール情報送信手段
50
D I / F
受信側認証手段
51
46

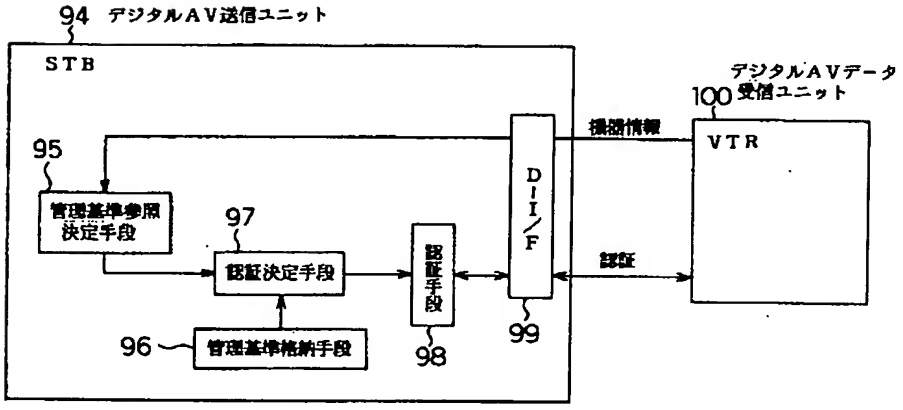
【図８】


93 デジタルAV送信ユニット
STB
データ
85
データ重要性判定手段
86
87
管理基準参照決定手段
89
認証決定手段
88
管理基準格納手段
認証手段
90
D I / F
91
認証
デジタルAVデータ
92 受信ユニット
TV

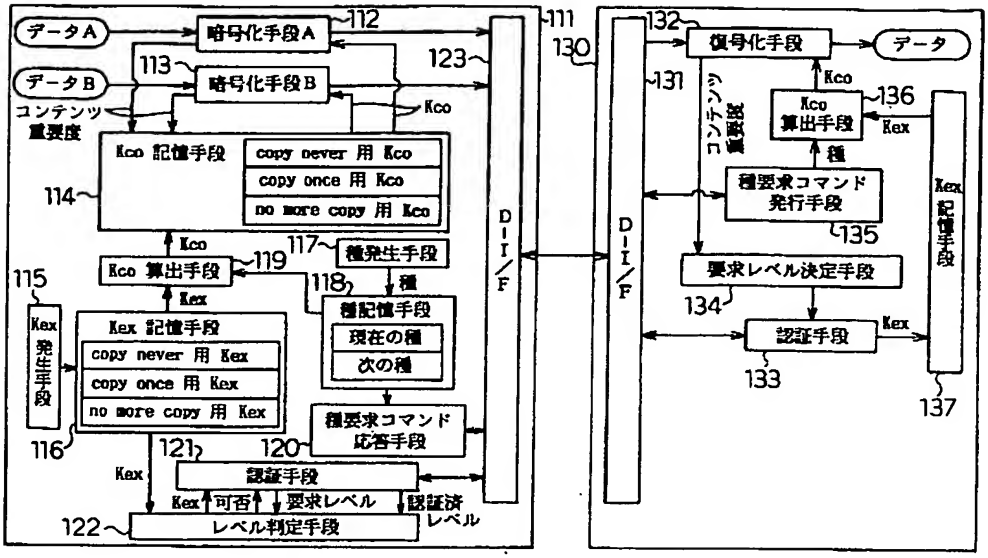
【図７】


STB
Kco
79
データ
暗号化手段
64
データ重要性判定手段
57
送信側複数認証ルール格納手段
63
61
58
送信側認証ルール取り出し手段
ユニット認証ルール情報受信手段
60
送信側認証手段
送信側認証選択手段
59
62
D I／F
暗号化データ
認証要求
認証
認証要求
認証
認証ルール関連情報送信
82
56
デジタルＡＶデータ送信ユニット
TV
80
Kco
66
復号化手段
83
データ
67
認証要求手段
65
複数認証デジタルＡＶデータ受信ユニット
D I／F
受信側認証手段
68
受信側複数認証ルール格納手段
69
受信側認証選択手段
70
71
VTR
81
Kco
73
復号化手段
データ
認証要求手段
84
D I／F
受信側認証手段
74
75
受信側認証ルール格納手段
76
認証ルール情報送信手段
77
72
78
単一認証デジタルＡＶデータ受信ユニット

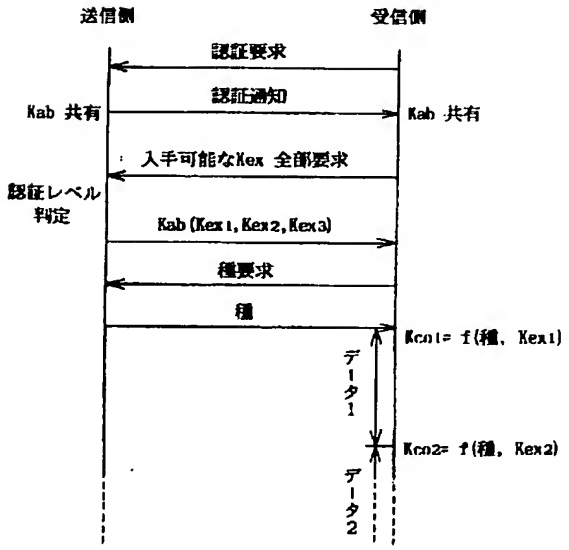
【図９】


94
デジタルＡＶ送信ユニット
STB
デジタルＡＶデータ受信ユニット
100
機器情報
VTR
95
管理基準参照決定手段
97
認証決定手段
認証手段
D I／F
認証
96
管理基準格納手段
98
99

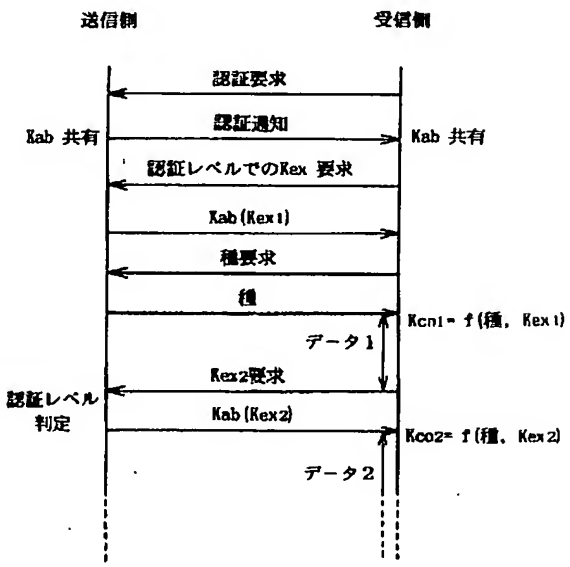
【図１０】


データA
暗号化手段A
112
データB
暗号化手段B
113
123
コンテンツ重要度
Kco
Kco 記憶手段
copy never 用 Kco
copy once 用 Kco
no more copy 用 Kco
114
Kco 算出手段
119
117
種発生手段
種
115
Kex
Kex 発生手段
Kex 記憶手段
copy never 用 Kex
copy once 用 Kex
no more copy 用 Kex
116
種記憶手段
現在の種
次の種
種要求コマンド応答手段
120
121
認証手段
可否
要求レベル
認証済レベル
122
レベル判定手段
D I / F
111
130
132
復号化手段
データ
131
コンテンツ認識
Kco 算出手段
136
種要求コマンド発行手段
135
要求レベル決定手段
134
認証手段
133
Kex 記憶手段
137

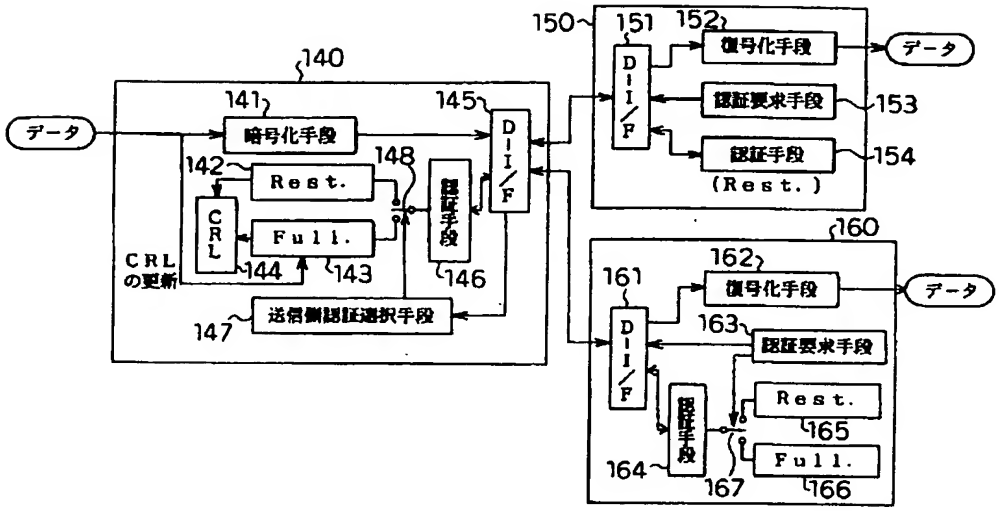
【図１１】


送信側
受信側
認証要求
認証通知
Kab 共有
Kab 共有
入手可能なKex 全部要求
認証レベル判定
Kab (Kex1, Kex2, Kex3)
種要求
種
Kco1= f(種, Kex1)
データ1
Kco2= f(種, Kex2)
データ2

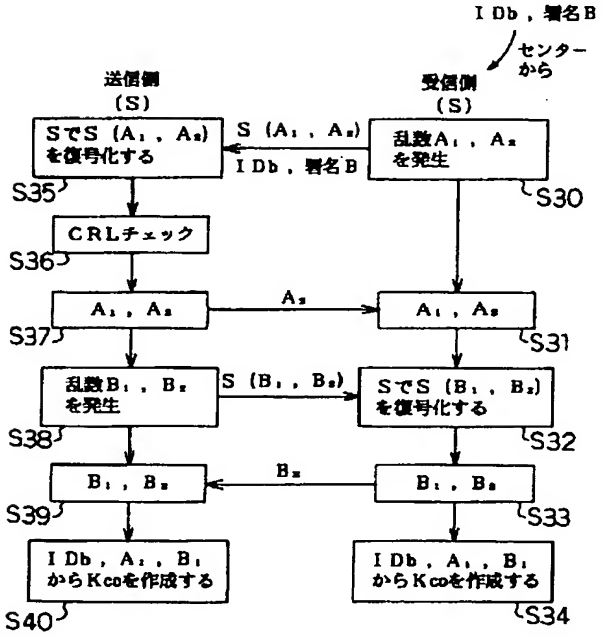
【図１２】


送信側
受信側
認証要求
認証通知
Kab 共有
Kab 共有
認証レベルでのKex 要求
Kab (Kex1)
種要求
種
Kco1= f(種, Kex1)
データ1
Kex2要求
認証レベル判定
Kab (Kex2)
Kco2= f(種, Kex2)
データ2

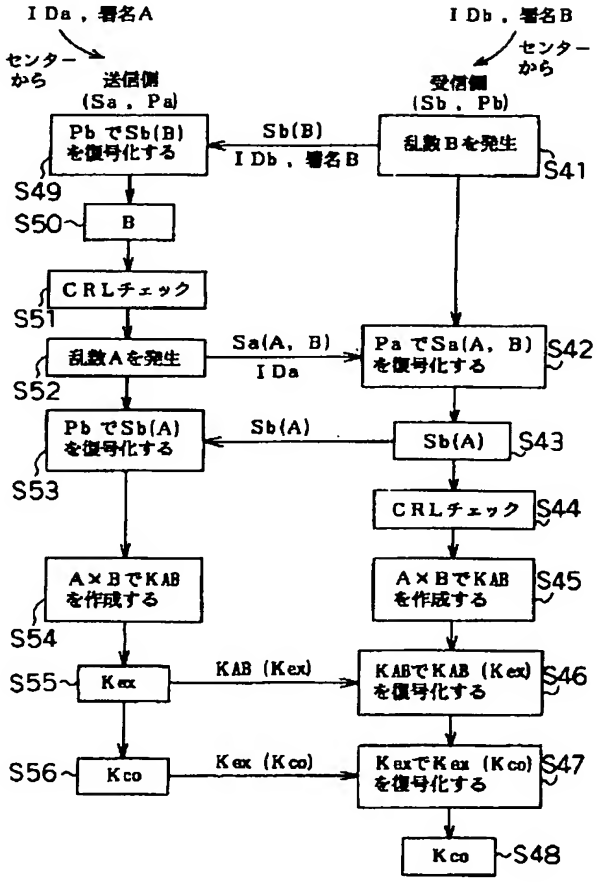
【図１３】


150
151
152
復号化手段
データ
D I / F
認証要求手段
153
認証手段
154
(Rest.)
140
141
暗号化手段
145
データ
D I / F
142
Rest.
148
CRL
Full.
認証手段
CRL の更新
144
143
146
147
送信側認証選択手段
160
162
161
復号化手段
データ
D I / F
163
認証要求手段
Rest.
165
認証手段
164
167
Full.
166

【図１４】


I Db，署名B
センターから
送信側 (S)
受信側 (S)
SでS (A1，A2) を復号化する
S (A1，A2)
I Db，署名B
乱数A1，A2を発生
S35
S30
CRLチェック
S36
A1，A2
A2
A1，A2
S37
S31
乱数B1，B2を発生
S (B1，B2)
SでS (B1，B2) を復号化する
S38
S32
B1，B2
B2
B1，B2
S39
S33
I Db，A1，B1からKcoを作成する
I Db，A1，B1からKcoを作成する
S40
S34

【図１５】


I Da，署名A
センターから
送信側 (Sa，Pa)
I Db，署名B
センターから
受信側 (Sb，Pb)
Pb でSb(B) を復号化する
Sb(B)
I Db，署名B
乱数Bを発生
S49
S41
S50
B
CRLチェック
S51
乱数Aを発生
Sa(A，B)
I Da
Pa でSa(A，B) を復号化する
S42
S52
Pb でSb(A) を復号化する
Sb(A)
Sb(A)
S43
S53
CRLチェック
S44
A×BでKABを作成する
A×BでKABを作成する
S45
S54
S55
Kex
KAB (Kex)
KABでKAB (Kex) を復号化する
S46
S56
Kco
Kex (Kco)
KexでKex (Kco) を復号化する
S47
Kco
S48

フロントページの続き

(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　後藤　昌一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　武知　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　臼木　直司
大阪府門真市大字門真1006番地　松下電器産業株式会社内